UNITED STATES

DEPARTMENT OF THE TREASURY

DEPARTMENT OF THE TREASURY (DOT)

PUBLIC KEY INFRASTRUCTURE (PKI)

X.509 CERTIFICATE POLICY

VERSION (RFC 3647) 2.0

January 2, 2008

UNCLASSIFIED

SIGNATURE PAGE

/s/ _____

PKI Policy Management Authority

_____

DATE

DOCUMENT VERSION CONTROL

Version	Date	Author(s)	Description	Reason For Change
2.0	January 2008	James Schminky	Department of the Treasury PKI Policy in RFC 3647 format.	Bring the Treasury PKI Policy into compliance with FPKIPA change proposal requiring all cross certified PKI Policies to be in RFC 3647 format.

TABLE OF CONTENTS

TABLE OF TABLES

1. INTRODUCTION

Note: The term "policy" is used in this document in the context of X.509 Certificate Policy (CP) as opposed to how the term "policy" is generally used at the Department of the Treasury.

The United States Department of the Treasury (DoT[1]) has implemented a Public Key Infrastructure (PKI) that provides a method for securing transmission of information across Department Automated Information System (AIS) assets, and supports the verification of an individual's identity for physical and logical access control. Overall, the PKI Program establishes a secure electronic environment, at the Sensitive But Unclassified (SBU) level, that fully complements hard-copy documentation standards currently in use. This Certificate Policy (CP) defines the minimum standards necessary to implement and manage the PKI architecture, identifies a PKI Program Team, and details the Department's program.

A PKI consists of products and services that provide and manage X.509 certificates for public key cryptography. Public key cryptography is an information technology security service that can provide identity authentication, data integrity, technical non-repudiation, and confidentiality (i.e., privacy) to electronic transactions.

This CP defines six certificate policies for use by the Department of the Treasury PKI X.509 Certification Authorities (CAs) to facilitate interoperability between the DoT PKI domain and the Federal Bridge Certification Authority (FBCA), the Federal Common Policy Framework (FCPF), the Citizen and Commerce Class Common Certification Authority (C4CA), and other Entity PKI domains. The policies represent four different assurance levels (Rudimentary, Basic, Medium, and High) for public key certificates. The level of assurance refers to the strength of the binding between the public key and the individual whose subject name is cited in the certificate, the mechanisms used to control the use of the private key, and the security provided by the PKI itself.

All subordinate CA certificates contain a NIST-registered Certificate Policy Object Identifier (OID), which a Relying Party may use to decide whether a certificate is trusted for a particular purpose. The OID corresponds to a specific level of assurance established by this CP. In addition, the DoT PKI, under the SSP, will issue certificates with OIDs that correspond to a specific level of assurance established by FCPF. Each end-entity or subordinate certificate issued by the Department will assert the appropriate levels of assurance in the *certificatePolicies* extension. Any use of or reference to this CP outside the purview of the Department of the Treasury PKI Policy Management Authority (PMA) is completely at the using party's risk. An Entity outside the Department of the Treasury shall not assert the DoT PKI CP OIDs in any certificates the Entity CA issues, except in the *policyMappings* extension establishing an equivalency between a DoT PKI CP OID and an OID in that Entity CA's CP.

This CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (PKIX) RFC 3647, "Certificate Policy and Certification Practices Framework." Users

[1] The "DoT" acronym used in this document refers to the Department of the Treasury as an entity, and should not be confused with the term "DoT PKI," which is a naming convention used by the Department to include all non-specialty PKIs operating within the Department. This document applies *only* to the DoT PKI.

shall interpret the terms and provisions of this CP under and be governed by applicable Federal law. This policy is also in consonance with and augments the information system security requirements in Treasury Department Publication (TD P) 85-01, "Treasury IT Security Program", Appendices C.

The reliability of the public key cryptography portion of the security solution is a direct result of the secure and trustworthy operation of an established PKI, including equipment, facilities, personnel, and procedures. This CP applies to all the components of the Treasury Certification Authority (TCA)[2], for Trusted Roles such as Security Officers, Administrators, Auditors, Operators, Registration Authorities (RAs), Local Registration Authorities (LRAs), Trusted Agents (TAs), who support the trusted operations of the TCA, and certificates issued to Federal employees, contractors, and other affiliated personnel for the purposes of authentication, signature, and confidentiality. The Subscriber policies require Federal employees, contractors, and other affiliated personnel to use Federal Information Processing Standards Publication (FIPS Pub) 140 validated cryptographic modules for cryptographic operations and the protection of trusted public keys. The device policy also requires use of FIPS Pub 140 validated cryptographic modules for cryptographic operations and the protection of trusted public keys.

1.1 OVERVIEW

1.1.1 Certificate Policy

The United States Department of the Treasury *Public Key Infrastructure X.509 Certificate Policy* (DoT PKI CP) is the policy under which the Department establishes and operates the Treasury Root Certification Authority (TRCA) and any subordinate Certification Authorities[3]. The CP defines four distinct assurance levels for use by the DoT PKI CAs. Relying parties may base the reliance they choose to place on a given level of certificate assurance on the following:

- Amount and type of inherent risk of an activity
- Consequence of failure
- Use of risk mitigation controls

This document does not define certificate policy for CAs operated by external entities that communicate with the Department, and who issue their own certificates.

In addition, this document defines the creation and management of X.509, version 3, public key certificates for use in applications requiring trusted communication between networked computer-based systems. Such applications include, but are not limited to the following

[2] Treasury Bureaus may have existing unsanctioned, non-FBCA interoperable CAs that are not subordinate to the TRCA. These CAs are not considered part of the Federally approved cross-certified Treasury Certification Authority.

[3] Within this policy, the generic term “DoT PKI” refers to any and all PKI infrastructures operated by the Department of the Treasury. Unless otherwise specified, the term “TCA” generally refers to all PKI related hardware and software operating under the Treasury Certification Authority architecture; the term “SSP” generally refers to all PKI Certificate Authorities operating under the Common Policy Share Services Program architecture.

examples: electronic mail; transmission of SBU and/or classified information[4] on the appropriate networks, signature of electronic forms; contract submission signatures; and authentication of infrastructure components such as web servers, firewalls, directories, and mobile code. The Department of the Treasury also issues PKI certificates to authenticate the personal identity and validity of PIV credentials issued to Department employees, contractors, and other affiliated personnel in the United States for access to U.S. Government facilities and information systems by means of the PIV credential.

1.1.2 Relationship between the DoT PKI CP & the DoT PKI CA CPSs

The Department of the Treasury PKI CP states what assurance Subscribers can place in a certificate issued by the TCA. The Department of the Treasury CAs, including the SSP CAs, Certification Practices Statements (CPSs) state how each Root and subordinate CAs establish that assurance.

1.1.3 Relationship between the DoT PKI CP and the FBCA and Other Entity CPs

The Federal PKI Policy Authority (FPKIPA) maps levels of assurance between the FBCA and various Entity CAs to facilitate interoperability. The DoT PKI X.509 CP is consistent with the FBCA CP and applicable portions of the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework (a.k.a. Common Policy or COMMON).

In the same manner that the FPKIPA maps the FBCA CP to the DoT PKI X.509 CP, the DoT PMA maps other Entity CPs to the levels of assurance in the DoT PKI X.509 CP. The PMA will approve the acceptance of external CPs for cross certification to the Department of the Treasury TRCA, based on the recommendations of the PKI Operating Authority, the PKI Program Management Office, and any respective assurance mapping levels determined by the FPKIPA. The Department of the Treasury TRCA asserts the relationship between these CPs and the CA in the *policyMappings* extension of the CA certificates issued by the TRCA. The only exception to this rule is the relationship between the DoT PKI X.509 CP and those of other Entities that are also cross certified with the FBCA. The DoT PMA will generally accept the assurance level mapping determinations of the FPKIPA.

1.1.4 Scope

This CP applies to certificates issued to CAs, devices, and Federal employees, contractors, and other affiliated personnel. This CP also applies to certificates issued to organizations and/or groups of people, with the understanding that such certificates, by the nature of such use, lose the capacity for technical non-repudiation.

The TCA exists to facilitate trusted electronic business transactions for Treasury organizations. Programs that carry out or support this mission require services such as authentication, confidentiality, data-integrity, technical non-repudiation, and logical access control. An array of network security components, such as workstations, guards, firewalls, routers, and trusted database servers, satisfy these service requirements. The use of public key cryptography

[4] The existence and use of PKI does not authorize or permit the transmission of classified information over unclassified networks.

supports and complements the operation of these components. This CP implements a level of assurance comparable to the FBCA High Assurance Policy, and all lower assurance levels. Services provided by the PKI include:

- Key Generation/Storage/Recovery
- Certificate Generation, Update (i.e., Key Recovery),Renewal, Re-key, and Distribution
- Certificate Revocation List (CRL) and Authority Revocation List (ARL) Generation and Distribution
- Directory Management of certificate related items
- Certificate token initialization/programming/management
- System Management Functions (e.g., security audit, configuration management, archive)

Defining requirements on PKI activities, including the following, ensures the security of these services:

- Subscriber identification and authorization verification
- Control of computer and cryptographic systems
- Operation of computer and cryptographic systems
- Usage of keys and public key certificates by Subscribers
- Definition of rules to limit liability and to provide a high degree of certainty

1.1.5 Interaction with PKIs External to the Federal Government

The Treasury TRCA achieves interoperation with non-Federal CAs that issue under different policies by policy mapping and cross certification through the FBCA, the FCPF, the C4CA, or directly with the agency in question. The TRCA will extend interoperability with non-Federal entities only when it is beneficial to the Federal Government and to the mission of the Department.

1.2 DOCUMENT IDENTIFICATION

The official title of this CP is the *U.S. Department of the Treasury Public Key Infrastructure X.509 Certificate Policy*. The Treasury Root Certificate Authority (TRCA) operates at four (4) levels of assurance authorized to assert multiple policy object identifiers to specify the intended purpose of the certificate. There are six policies specified at four levels of assurance in this Certificate Policy. Subsequent sections of this document define the four levels of assurance asserted by this policy. Each level of assurance has an OID for the CP, asserted in certificates issued by CAs within the TCA. The National Institute of Standards and Technology (NIST) assigned the following IETF notation arc for DoT CPs: 2.16.840.1.101.3.2.1.5.

International Organization for Standardization (ISO) notation represents this as:

treasury-policies OBJECT IDENTIFIER: = {joint-iso-ccitt (2) country (16) us (840) organization (1) gov (101) csor (3) pki (2) cert-policy (1) treasury-policies (5) [X]}

The Department has registered the following certificate policies (in order of increasing assurance) in the NIST Computer Security Objects Registry under this arc:

Table 1-1, Certificate Policy OIDs

Certificate Policy	OID suffix
id-treasury-certpcy-rudimentary[5]	::= { treasury -policies [2] }
id- treasury-certpcy-basicIndividual[6]	::= { treasury -policies [3] }
id- treasury-certpcy-basicOrganizational	::={ treasury-policies [8] }
id- treasury-certpcy-medium[7]	::= { treasury-policies [7] }
id- treasury-certpcy-mediumHardware	::= { treasury-policies [4] }
id- treasury-certpcy-high	::= { treasury-policies [5] }

The Department may also assert the following certificate policy:

Table 1-2, Additional Certificate Policy OIDs

Certificate Policy	OID suffix
id-fpki-common-authentication	::= {2.16.840.1.101.3.2.1.3.13}

Certificates issued to subscribers supporting PIV II (FIPS 201, FIPS 201-1) authentication, and not digital signatures shall contain the id-fpki-common-authentication OID to support eAuthentication. The id-fpki-common-authentication policy is identical to id-fpki-common-hardware, excepting for the key usage constraints as mentioned in FCPF.

Federal PKI policy reserves the High Assurance policy for certificates issued and used between government (federal, state, and local) entities. The requirements associated with the Medium Hardware policy are identical to those defined for the Medium Assurance policy; with the exception of Subscriber cryptographic module requirements (see Section 6.2.1). The appropriate TRCA or subordinate CA CPS specifies which policy OIDs that CA asserts.

[5] DoT previously referred to the Rudimentary Assurance level by the common name “Level 1” for internal Department clarity.
[6] DoT previously referred to the Basic Assurance level by the common name “Level 2” for internal Department clarity.
[7] DoT previously referred to all Medium Assurance level certificates by the common name “Medium Assurance” for internal Department clarity.

The DoT PKI X.509 CP does not assert Citizen and Commerce Class Common Certification Authority (C4CA) certificates or Medium and Medium Hardware Commercial Best Practice (Medium-CBP and MediumHW-CBP) policies.

1.3 PKI ENTITIES

The Assistant Secretary for Information Management and Chief Information Officer (CIO) assigned responsibility for the Department of the Treasury PKI Program to the Associate Chief Information Officer (ACIO) for E-Government. The following are roles relevant to the administration and operation of all DoT PKI CAs.

1.3.1 PKI Authorities

The Associate Chief Information Officer (ACIO) for E-Government is responsible for funding PKI, management of the PKI investment, and validation of PKI hardware and software through the PKI Program Management Office (PKI PMO). The Treasury PMA established this CP under the authority, and with the approval, of the DoT CIO.

1.3.1.1 Treasury Policy Management Authority

The Treasury Policy Management Authority (PMA) resides in the Office of Cyber Security, Office of the Chief Information Officer (OCIO) for the Department of the Treasury. The PMA provides management authority over the Department's PKIs. As such, the PMA ensures the conformity to central Department policy for PKI implementation and operation to ensure installation of one PKI solution throughout the Department. The PMA is responsible for:

- The Treasury PKI Policy (CP);
- Review, approval and compliance review of all Treasury CPSs issued and maintained in support of the Treasury Certification Authority (TCA);
- Approval of any subordinate or other certificate authorities created in support of other Agencies and Bureaus to support digital technologies for authentication, signing, encryption, access, or authorizations;
- Oversight compliance management of the TCA and all Treasury CAs signed by the TRCA;
- Internal Auditing and compliance oversight of TCA operations;
- Determinations regarding CP and CPS compliance and assurance level with the Department of the Treasury CP;
- Review and approval of Treasury or other Entities CPs and CPSs pertaining to CAs being considered for cross certification with the TRCA.

In the event the PMA makes the determination that other, non-Department of the Treasury Certificate Policies offer appropriately equivalent levels of assurance to the Department of the Treasury Certificate Policies. The TCA may respond to such decisions by methods including but not limited to the following:

- Issuing cross certificates to other PKIs asserting other policies
- Including certificates issued by other PKIs and asserting other Certificate Policies, in Department of the Treasury Certificate Status Authorities (CSAs)
- Recommending CAs asserting other Certificate Policies for inclusion in Department of the Treasury application trust lists

The PMA shall make information regarding such equivalency determinations widely available to Department of the Treasury Subscribers and Relying Parties.

1.3.1.2 Treasury PKI Program Management Office (PMO)

Under the ACIO, the Director of Enterprise Solutions has oversight responsibilities for the PKI Program. The Director of Enterprise Solutions, has vested day-to-day management authority in the PKI Program Management Office (PMO).

The PMO enforces this policy and represents the interests of the PKI Program and the Department in all internal and external matters relative to PKI technology. The PMO is responsible for the following:

- Managing the operation and maintenance of the TCA on behalf of the Department of the Treasury;
- Creation, publication and maintenance of all CPSs pertaining to the Department of the Treasury PKI;
- Reviewing applications from Entities desiring to interoperate using the TRCA;
- Publishing this CP and coordinating modifications to ensure continued compliance by all DoT PKI CMAs operating under approved CPSs;
- Overseeing implementation of corrective actions or other measures as appropriate;
- Bureau RA and LRA training;
- Bureau RA and LRA guidance.

1.3.1.3 PKI Operational Authority

The CIO has designated the Bureau of Public Debt, as the PKI Operational Authority (PKI OA). The PKI OA is responsible for the operation, and control of the Treasury TRCA and the operation, control and management of all subordinate CAs. In addition, the PKI OA is responsible for the following:

- Establishing the operational requirements for the subordinate CAs in the CPSs

- Making recommendations to the PMO and PMA regarding corrective actions or other measures that might be appropriate for the TCA.

The PKI OA established the PKI Program Team. The PKI Program Team is the organization that operates and maintains the DoT PKI CAs on behalf of the Department of the Treasury, subject to the direction of the PMA.

1.3.1.4 PKI Program Manager

The PKI Program Manager is the individual within the PKI Program Team who has principal responsibility for overseeing the proper operation of the DoT PKI CAs on a daily basis, including the respective CA repositories and selecting the Operational Authority staff. The Program Manager is selected by and reports to the PKI OA.

1.3.1.5 PKI Program Team

The PKI Program Team has the following responsibilities:

- Administer the Department's PKI from an operational perspective, including[8]:
  - Publication of certificates;
  - Perform issuance and revocation of certificates to subordinate CAs, and to Subscribers from those CAs;
  - Manage certificate repositories and certificate and authority revocation lists;
  - Ensure that all aspects of CA services, operations and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP, the appropriate CPS, and Department policy.
- Manage technical operational issues, including:
  - Set up and administer subordinate CAs;
  - Implement the PKI and components;
  - Coordinate installation;
  - Administer the Department's PKI from a key management perspective, including re-key of CA signing material in cooperation with the PMO;
- Create and revise Certification Practices Statements, including evaluation of changes at the requested of the PMA or PMO, and recommendation for approval/disapproval to the PMA, to maintain the level of assurance and operational practicality;
- Establish operational policy and procedures for subordinate CAs;
- Perform Certification and Accreditation activities, including:

[8] To satisfy specific operational requirements, the PKI OA may designate DoT personnel outside the PKI Program Team (PKI PT) to fulfill certain functions including some, but not necessarily all, of the functions listed hereunder. These personnel must satisfy all of the same qualifications as PKI PT personnel appointed to the same function.

- Preparation of system security plans
- Conduct annual system security self-assessment reviews and prepare Plans of Action and Milestones
- Perform Backup and Contingency planning, including:
- System backup
- Key recovery
- Key escrow
- Disaster recovery planning
- Perform contingency planning to ensure continuity of operations
- Participate in the Federal PKI Policy Authority Share Service Program working group to ensure compliance to the Federal model
- Conduct liaison with other government agencies concerning SSP PKI matters
- Act as a focal point for DoT participation in the Federal PKI Policy Authority SSP

1.3.1.6 Root Certification Authority

The TRCA (the collection of hardware, software, and operating personnel) is established by the PMO to certify subordinate CAs that, in turn, create, sign, and issue public key certificates to subscribers within DoT and other related PKI communities. The Department's PKI operates in a hierarchical fashion, utilizing a TRCA and subordinate CAs. The TRCA serve as the trust anchors for all certificates issued under this policy. The TRCA also act as the Principal CA (PCA) for DoT to cross certify directly with the FBCA (e.g., through the exchange of cross certificates).

The Principal CA issues either end entity certificates, or CA certificates to other Entity or external party CAs, or both. The PCA shall cross certify with the FBCA, and other root level CAs from other trust domains as appropriate. The PCA shall also certify CA's within DoT that want to be part of the subordination hierarchy (as opposed to cross certification).

This policy permits an off-line TRCA. The TRCA shall be physically isolated from all networks. The TRCA is responsible for issuing and managing certificates; and ensuring that the performance of all aspects of CA services, operations, and infrastructure related to certificates issued under this policy are in accordance with the requirements, representations, and warranties of this policy. This includes the following:

- The TRCA certifies subordinate CAs, which will assert one or more assurance levels defined in this CP, and outlined in the appropriate CPS
- The TRCA shall also comply with the requirements set forth in applicable Memorandum of Agreement (MOA), Memorandum of Understanding (MOU), and contractual agreements with cross certified CAs and/or other entities

1.3.1.7 Subordinate Certification Authorities

Subordinate CAs are responsible for all aspects of the issuance and management of a certificate to users and devices, including control over the enrollment process, the identification and authentication process, the certificate manufacturing process, publication of certificates, revocation of certificates, and re-key.

A CA, which issues certificates that assert the policies defined in this document, shall conform to the stipulations of this document, including the following:

- Providing to the appropriate authorities a CPS, as well as any subsequent changes, for conformance assessment
- Maintaining its operations in conformance to the stipulations of the approved CPS
- Ensuring that registration information is accepted only from RAs/LRAs who understand and are obligated to comply with this policy, and operating under an approved CPS
- Including only valid and appropriate information in the certificate, and to maintaining evidence that due diligence was exercised in validating the information contained in the certificate
- Ensuring that all Subscribers (government and non-government) are informed of their obligations under Sections 1.4 and 9.6.3, including the consequences of not complying with those obligations, and revoking the certificates of Subscribers found to have acted in a manner counter to those obligations
- Operating or obtaining the services of an online repository that satisfies the obligations under Section 1 and Sections 9.6.1 and 9.6.5, and informing the repository service provider of those obligations if applicable

1.3.1.8 Certificate Status Servers

The TCA may optionally include an authority that provides status information about certificates on behalf of the DoT PKI CAs through online transactions. Examples include Online Certificate Status Protocol (OCSP) responders, termed Certificate Status Servers (CSS) identified in the Authority Information Access (AIA) extension. Where certificates identify the CSS as an authoritative source for revocation information, the operations of that authority are within the scope of this CP. This policy does not cover OCSP servers that are locally trusted, as described in RFC 2560.

1.3.2 Registration Authority/Local Registration Authority

The DoT Registration Authorities (RA), and Local Registration Authorities (LRA) are entities recognized as authorized to collect and verify users' identity and information which is to be entered into the Subscriber's public key certificates. The key difference between RAs and LRAs is the nature and degree of their respective access to the DoT PKI CAs. The RA, by definition, functions as the Officer trusted role of the DoT PKI CA as defined in Section 5.2.1.2. The PMO appoints RA(s) for Treasury TRCA from members of the PMO, PKI Program Team, or other

DoT personnel as necessary for specific operational requirements, and who perform their functions in accordance with a CPS approved by the PMA, as detailed in Section 1.3.1.5.

Both Certification Authorities and Registration Authorities are termed "Certificate Management Authorities (CMA)." This policy uses the term "CMA" when a function may be assigned to either a CA or an RA, or when a requirement applies to both CAs and RAs. The term "Registration Authority" includes entities such as Local Registration Authorities (a.k.a. Trusted Agents[9]), unless otherwise specified. Section 5.2.1, Trusted Roles, lists specifically defined trusted roles, i.e., roles whose incumbents perform functions that involve the handling of sensitive cryptographic material and can thus introduce security problems to the CA if not carried out properly.

The division of Subscriber registration responsibilities between the CA and RA may vary among implementations of this CP, as outlined in the appropriate CPS. All CMAs shall protect personal information from unauthorized disclosure as mandated by the Privacy Act of 1974, as amended.

1.3.3 Subscribers

A Subscriber is the Entity (the user to whom, or device to which, a certificate is issued) whose Distinguished Name (DN) appears as the subject in a certificate, and who asserts that it uses the key and certificate in accordance with this policy. Sometimes, a PKI technically considers CAs as "Subscribers." However, the term "Subscriber" as used in this document refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information. Department of the Treasury PKI Subscribers include but are not limited to the following categories of entities that may wish to conduct official Department business:

- Department of the Treasury personnel: Direct Hire, Part-time/Intermittent/Temporary (PIT) employees, contractors, commercial vendors, and agents
- Federal Government departments and agency personnel, and their contractors and agents
- Workstations, guards and firewalls, routers, trusted servers (e.g., database, domain controller, FTP, and WWW), and other infrastructure components. These components must be under the cognizance of humans, who accept the certificate and are responsible for the correct protection and use of the associated private key

A PKI Sponsor fills the role of a Subscriber for groups, organizations, disabled personnel, and non-human system components named as public key certificate subjects. The PKI Sponsor works with the CMAs to register the above elements in accordance with Section 3.2.2 and 3.2.3, and is responsible for meeting the obligations of Subscribers as defined throughout this document.

TRCA Subscribers include only PMA, PMO or PKI Program Team personnel and, when determined by the PMA, PKI network or hardware devices.

[9] A "Trusted Agent" is a person who satisfies all of the trustworthiness requirements for an RA, and who performs identity proofing as a proxy for the RA recording and verifying information about applicants as outlined in the applicable CPS and supporting Standard Operating Procedures.

The DoT may issue certificates to Subscribers other than employees of the U.S. Government, such as commercial vendors and agents, at the convenience of the Government and without fee, when those Subscribers have a bona fide need to possess a certificate issued by a DoT CA. The DoT shall inform such Subscribers of the stipulations of this policy by including the provisions of Section 9.6.3 in the Subscriber agreements. These Subscribers are under the same policy obligations as those specified for a DoT direct hire.

1.3.4 Relying Parties

A Relying Party uses a Subscriber's certificate to verify or establish:

- the identity and status of an individual
- the integrity of a digitally signed message
- the identity of the creator of a message
- confidential communications with the Subscriber

The Relying Party relies on the validity of the binding between the Subscriber's name and public key. A Relying Party may use information in the certificate (such as Certificate Policy Identifiers) to determine the suitability of the certificate for a particular use. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. For this Certificate Policy, the relying party may be any Entity that wishes to validate the binding of a public key to the name of a federal employee, contractor, other affiliated personnel or devise.

This CP makes no assumptions or limitations regarding the identity of Relying Parties. While Relying Parties may be Subscribers, Relying Parties are not required to have an established relationship with the DoT PKI CA, FBCA, or another Entity CA.

1.3.5 Other Participants

All CAs operating under this policy require the services of other security and application authorities, such as compliance auditors and attribute authorities. Each CA shall identify, in its CPS, the parties responsible for providing such services and the mechanisms used to support these services. Section 5.2 provides more detail on these authorities, services, and mechanisms.

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

The sensitivity of the information processed or protected using certificates issued by the TCA may vary significantly. Relying Parties should evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. Each Relying Party makes this evaluation for its application outside the control of this CP. To provide sufficient granularity, this CP specifies security requirements at five increasing, qualitative levels of assurance: Rudimentary, Basic, Medium, Medium Hardware, and High. The TRCA will issue at least one High assurance certificate, so the TRCA will operate at that level.

All DoT bureaus that use PKI technology to secure data are subject to the requirements of this policy. The TCA is intended to support applications involving unclassified information, which can include Sensitive But Unclassified (SBU) data protected pursuant to Federal statues and regulations. Other agencies that exchange information electronically with Department assets, including those requiring the security of Public Key technology, are subject to the same requirements. Each CA asserting this policy must state this requirement in the CPS and inform Subscribers of the limitation.

The level of assurance associated with a public key certificate describes the procedures and controls involved in validating a Subscriber's identity and binding that identity to a public key. It is the responsibility of the Relying Party to assess that level of assurance and determine if it meets their security requirements for some particular use. The level of assurance depends on the proper generation and management of the certificate and associated private keys, in accordance with the stipulations of this policy. Personnel, physical, procedural, and technical security controls contribute to the assurance level of the certificates issued by a certificate management authority or system.

The following table provides a brief description of the appropriate uses for certificates at each level of assurance defined in this CP. These descriptions are guidance and are not binding.

Table 1-3, Certificate Uses

Assurance Level	Appropriate Certificate Uses
Rudimentary	This level provides the lowest degree of assurance concerning identity of the individual. One of the primary functions of this level is to provide data integrity to the digitally signed information. This level is relevant to environments in which the risk of malicious activity is considered low. It is not suitable for transactions requiring authentication, and is generally insufficient for transactions requiring confidentiality, but may be used for the latter where certificates having higher levels of assurance are unavailable.
Basic	This level provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but which are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. This security level assumes that subscribers are not likely to be malicious.
Medium	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial.
Medium Hardware	This level is relevant to environments where threats to data are high or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.

Table 1-3, Certificate Uses

Assurance Level	Appropriate Certificate Uses
High	This level is reserved for cross certification with government entities and is appropriate for those environments where the threats to data are high, or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.

General usage for certificates covered by this policy includes:

- Digital signature services (authentication and data integrity)
- Protection (confidentiality)
- Technical non-repudiation
- Authentication of identity and status with the Department for access control to a Federal facility or information systems across the Federal Government

1.4.2 Prohibited Certificate Uses

Subscribers shall not use DoT PKI certificates to conceal an unauthorized act as specified in Federal law or Department of the Treasury regulations. Examples of such actions include, but are not limited to, the following:

- Use of PKI certificates, especially in conjunction with a DoT-issued PIV card, to gain unauthorized access to a Federal facility, information system, or electronic data (e.g., Privacy information), or to enable others to gain such access
- Use of PKI certificates to facilitate and/or hide an unauthorized action, such as:
  - Transfer information to an unauthorized individual
  - Generate income for oneself or for an organization
  - View sexually explicit material, gamble, or for the purposes of conducting unlawful or malicious activities
  - Negatively affect the integrity, accessibility, and/or confidentiality of the Department's cyber infrastructure

The DoT specifically prohibits such uses of PKI regardless of whether the use is during or outside normal work hours, whether use occurs on or off U.S. Government premises, or whether the use occurs within or outside the United States.

Each CA asserting this policy must state this requirement in the CPS and inform Subscribers of these usage limitations. All Department of the Treasury bureaus, offices, and posts that use PKI technology are subject to the requirements of this policy.

1.5 POLICY ADMINISTRATION

1.5.1 Organization administering the document

The PMA is responsible for all aspects of this CP.

1.5.2 Contact Person

Direct questions regarding this CP to Treasury PMA, at the following address:

U.S. Department of the Treasury, Suite 12000
1750 Pennsylvania Ave. N. W.
Washington, DC 20220
(202) 622-2446

1.5.3 Person Determining Certification Practices Statement Suitability for the Policy

Certification Practices Statements, derived from this CP, must conform to the corresponding requirements of this Certificate Policy. The PMO, shall determine the suitability of any CPS to this policy, and recommend approval to the PMA. In each case, the PMO and PMA shall base the determination of suitability on a compliance audit results and recommendations. See section 8 for further details.

1.5.4 CPS Approval Procedures

The PKI OA shall submit the TRCA CPS (and any separate subordinate CA CPS) to the PMO. The PMO will submit the CPS(es) and the results of a compliance audit, to the PMA for approval. The PMA shall accept or reject the CPSs. If rejected, the PMO and PKI OA shall resolve the identified discrepancies and resubmit to the PMA.

Waivers are not allowed. The Treasury PMA shall decide what variations in CMA practices are acceptable under this CP, or the CMA shall request a permanent change to this CP. Change proposals shall be submitted by the Treasury PMA/PMO to meet urgent, unforeseen operational requirements (such as those associated with unique operational activities, ongoing law-enforcement, and financial mission). When a change proposal is granted and approved by the Treasury PMA, the Treasury PMO shall post the change proposal on its web site which is accessible by interested or relying parties.

The PMA, shall notify the FPKIPA, and provide information regarding the specific provision changed, the rationale for the change, and either get approval or a request to submit the Department policy for re-cross certification.

1.6 DEFINITIONS AND ACRONYMS

See Appendices B and C

2. PUBLICATION & REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

The PKI Program Team shall operate repositories to support DoT PKI CA operations. The location of any publication will be one that is appropriate to the certificate-using community, and in accordance with the total security requirements of the Department. The PKI Program Team shall ensure interoperability with the FBCA repository[10].

The DoT PKI CA infrastructure will serve as the primary repository of information for Subscribers and Relying Parties. For all DoT PKI CAs, this repository is the DoT directory infrastructure. The PKI Program Team web site (http://pki.treas.gov) will serve as the primary repository to publish public information. Network directories and all other repositories used to disseminate relevant information will:

- Maintain availability necessary to distribute current certificate information in a manner consistent with the posting and retrieval stipulations of Section 2.2.1, and the appropriate CA CPS
- Implement access controls on all CA repositories to provide sufficient protection as described in Section 5.1.2

The PKI Program Team may use a variety of mechanisms for posting information into a repository as required by this CP. These mechanisms at a minimum shall include:

- A Directory Server System that is also accessible through the Lightweight Directory Access Protocol
- Availability of the information as required by the certificate information posting and retrieval stipulations of this CP
- Access control mechanisms when needed to protect repository information as described in later sections

2.2 PUBLICATION OF CERTIFICATION INFORMATION

2.2.1 Publication of Certificates and Certificate Status

TRCA and each subordinate CA in the TCA shall publish certificates and status information such that it is available over the publicly accessible network or other such networks appropriate to a particular "community of interest" and that includes the following:

- Issued certificates
- All CRL and ARL (each CA may also utilize an OCSP responder)
- The applicable CA certificates to validate a Subscriber certificate

[10] DoT PKI directories used for interoperating with the FPKIA directory shall use standard X.500 object classes and/or Entrust object classes (e.g., EntrustCA and EntrustUser). Use of other object classes must have FPKIPA approval. DoT PKI directories shall be configured such that the FPKI directory can obtain all necessary validation information using a single reference. Exceptions must have FPKIPA approval.

The PKI Program Team shall use only repository mechanisms (directory, certificate status server (CSS)) and procedures designed to ensure CA certificates and CRLs are available for retrieval 24 hours a day, 7 days a week, with a minimum of 99% availability overall per year and scheduled down-time not to exceed 0.5% annually[11].

2.2.2 Publication of CA Information

The PKI Program Team shall publish information concerning the DoT PKI necessary to support its use and operation. The PMO shall publish information (including this policy) on a web site, consistent with Department of the Treasury policies regarding web site contents, that is available to Subscribers and relying parties. Due to sensitivity, the Department will not publish any DoT PKI CA CPS.

2.2.3 Interoperability

Where the TCA publishes certificates and CRLs in directories, the directories shall use standards-based schemas whenever possible for directory objects and attributes in accordance with technical guidance from the FPKI Operational Authority (see http://www.cio.gov/fbca).

2.3 FREQUENCY OF PUBLICATION

The PMA shall make this CP and any subsequent changes publicly available within 30 days of approval.

The appropriate DoT PKI CA will publish certificates following user acceptance as specified in Section 4.4 and proof of possession of private key as specified in Section 3.2.1. Section 4.9 specifies publication requirements for CRLs. The CA shall publish all information normally published in the repository promptly after such information becomes available. Each PKI CA CPS specifies time limits within which it publishes various types of information.

2.4 ACCESS CONTROLS ON REPOSITORIES

Access to information in TCA repositories shall be determined by the PMO pursuant to the rules and statutes that apply. The DoT PKI OA shall protect any repository information not intended for public dissemination or modification. Public key certificates and certificate status information in a TCA repository shall be publicly available through the Internet wherever reasonable. At a minimum, the TCA repositories shall make CA certificates and CRLs issued by the TCA and CA certificates issued to the TCA available to Federal Relying Parties.

The appropriate CPS will detail what information in the repository shall be exempt from automatic availability and to whom, and under what conditions the PMO may make restricted information available.

[11] Where repository systems are distributed, the availability figures apply to the system as a whole, rather than each component; and availability targets exclude network outages.

3. IDENTIFICATION & AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

All DoT CAs shall be able to generate and sign certificates that contain an X.501 Distinguished Name (DN) or if applicable a Domain Component (DC) identifier.

For legacy Treasury employees, the DN will be of the following form:

"CN=userID, OU=bureau, OU=Department of the Treasury, OU=structural container, O=U.S. Government, C=US"

The organizational unit *bureau* and *Department of the Treasury* are used to specify the federal entity that employs the subscriber. At least one of these organizational units must appear in the DN. The additional organizational unit *structural container* is permitted to support local directory requirements, such as differentiation between human subscribers and devices. This organizational unit may not be employed to further differentiate between subcomponents within a bureau.

The userID is unique across the Treasury directory. It is a non-identifying ID and can be composed in the following form: the first two letters of the subscribers surname and a four digit number that is assigned sequentially as userID are assigned. The directory can be queried using a subscriber name (as long as access controls are not in place to protect it) or userID to get the subscriber's certificate.

For non-human Subscribers, a PKI Sponsor must provide a uniquely identifying name for the entity to be issued a certificate. This information may be a URL, IP address, hostname, application or process name, or other value that can reasonably identify this equipment. The name of the PKI sponsor does not need to appear in the certificate, but may be kept as an attribute in the directory. An example of a non-human subject would be:

CN =www.publicdebt.ustreas.gov, OU=Bureau of Public Debt, OU=Department of the Treasury, O=U.S. Government, C=US

The TCA was implemented before 2004 and is considered a "Legacy PKI" and therefore may use the existing directory tree schema while in transition to the directory schemas defined below. Common name fields will be populated as specified below for Federal and Contractor employees.

For certificates issued under policies associated with Medium (Software), Medium (Hardware), High, and for devices, the TCA shall generate and sign certificates that contain an X.501 DN. These distinguished names may be in either one of two forms: a geo-political name space or an Internet domain component (dc) name space. Where Subscriber certificate name forms must assert the FCPF (e.g., for PIV), Subscriber DNs shall also meet that policy.

The organizational units *department* and *agency* appear when applicable and are used to specify the federal entity that employs the subscriber. At least one of these organizational units must appear in the DN. The additional organizational unit *structural_container* is permitted to support local directory requirements, such as differentiation between human subscribers and devices. This organizational unit may not be employed to further differentiate between subcomponents within an agency.

All geo-political X.501 distinguished names assigned to Federal employees are in one of the following directory information trees:

C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou= *structural_container*]
C=US, [o=*department*], [ou=*agency*], [ou= *structural_container*]

All new implementations (after May of 2006) shall assign names in the following directory tree:

C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou= *structural_container*]

The organizational units *department* and *agency* appear when applicable and are used to specify the TCA Sponsor that employs the subscriber. At least one organizational unit must appear in the DN. The distinguished name of the Federal employee subscriber shall be structured in one of the three following forms:

1. C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou= *structural_container*], cn=nickname lastname
2. C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou= *structural_container*], cn=*firstname initial. lastname*
3. C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou= *structural_container*], cn=*firstname middlename lastname*

In the first name form (for both Federal or Contractor employees), *nickname* may be the subscriber's actual first name, a form of their first name, middle name, or pseudonym (e.g., Chuck for Charles) by which the subscriber is generally known.

X.501 distinguished names assigned to Federal contractors and other affiliated persons shall be within the same directory information tree. The distinguished name of the Federal contractor subscriber and any affiliate subscribers must take one of the three following forms:

1. C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou= *structural_container*], cn=*nickname lastname* (affiliate)
2. C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou= *structural_container*], cn=*firstname initial. lastname* (affiliate)
3. C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou= *structural_container*], cn=*firstname middlename lastname* (affiliate)

Distinguished names based on Internet domain component (dc) names shall be in one of the following directory information trees:

dc=gov, dc=*org0*, [dc=*org1*], [dc=*orgN*]
dc=mil, dc=*org0*, [dc=*org1*], [dc=*orgN*]

The default Internet domain name for any TCA participating component using either the [*orgN*.]…[*org0*].gov or [*orgN*.]…[*org0*].mil branches shall be used to determine DNs uniqueness. The first domain component of the DN shall be dc=gov or dc=mil. At a minimum, the *org0* domain component must appear in the DN. The *org1* to *orgN* domain components appear, in order, when applicable and are used to specify the Treasury entity that employs the subscriber.

The distinguished name of the TCA Federal employee subscriber must take one of the following three forms when the TCA Sponsor's Internet domain name ends in .gov:

1. dc=gov, dc=*org0*, [dc=*org1*], [dc=*orgN*], cn=*nickname lastname*
2. dc=gov, dc=org0, [dc=org1], [dc=orgN], cn=*firstname initial. lastname*
3. dc=gov, dc=org0, [dc=org1], [dc=orgN], cn=*firstname middlename lastname*

The distinguished name for Federal contractors and affiliated subscribers must use one of the following three forms when the TCA Sponsor's Internet domain name ends in .gov:

1. dc=gov, dc=org0, [dc=org1], [dc=orgN], cn=*nickname lastname* (affiliate)
2. dc=gov, dc=org0, [dc=org1], [dc=orgN], cn=*firstname initial. lastname* (affiliate)
3. dc=gov, dc=org0, [dc=org1], [dc=orgN], cn=*firstname middlename lastname* (affiliate)

The distinguished name of the Federal employee subscriber must use one of the following three forms when the TCA sponsor's Internet domain name ends in .mil:

1. dc=mil, dc=org0, [dc=org1], [dc=orgN], cn=*nickname lastname*
2. dc=mil, dc=org0, [dc=org1], [dc=orgN], cn=*firstname initial. lastname*
3. dc=mil, dc=org0, [dc=org1], [dc=orgN], cn=*firstname middlename lastname*

The distinguished name of the Federal contractors and affiliated subscribers must use one of the following three forms when the TCA sponsor's Internet domain name ends in .mil:

1. dc=mil, dc=org0, [dc=org1], [dc=orgN], cn=*nickname lastname* (affiliate)
2. dc=mil, dc=org0, [dc=org1], [dc=orgN], cn=*firstname initial. lastname* (affiliate)
3. dc=mil, dc=org0, [dc=org1], [dc=orgN], cn=*firstname middlename lastname* (affiliate)

The CA may supplement any of the name forms for users specified in this section by including a dnQualifier, serial number, or user id attribute. When any of these attributes are included, they may appear as part of a multi-valued relative distinguished name (RDN) with the common name or as a distinct RDN that follows the RDN containing the common name attribute. Generational qualifiers may optionally be included in common name attributes in distinguished names based on Internet domain names. For names assigned to employees, generational qualifiers may be

appended to the common name. For names assigned to federal contractors and other affiliated persons, generational qualifiers may be inserted between *lastname* and "(affiliate)". Sponsored devices that are the subject of certificates shall be assigned either a geo-political or an Internet domain component name. Device names must use one of the following forms:

C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], cn=*device name*
dc=gov, dc=*org0*, [dc=*org1*], [dc=*orgN*], [cn=*device name*]
dc=mil, dc=*org0*, [dc=*org1*], [dc=*orgN*], [cn=*device name*]

Where *device name* is a descriptive name of the device, and when a device is fully described by the Internet domain name, the common name attribute is optional.

Treasury CAs and CSSs distinguished names shall be either a geo-political or an Internet domain component name. The TCA will use the following naming convention for certificate authorities:

C=US, o=U.S. Government, ou=Department of the Treasury, ou=Certification Authorities, cn= [*CA name*]

A TCA participant or sponsoring entity reserves the right to issue certificates using any of the above-defined naming conventions in order to prevent duplication of Subscriber names to maintain uniqueness within the domain.

The table below summarizes the naming requirements that apply to each level of assurance.

Table 3-1, Naming Requirements

Assurance Level	Naming Requirements
Rudimentary	Non-Null Subject Name, or Null Subject Name if Subject Alternative Name is populated and marked critical
Basic	Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical
Medium (all policies)	Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical
High	Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical
PIV Authentication	Subject Alternative Name that include a name of type pivFASC-N, and option non-NULL Subject Name

3.1.2 Need for Names to Be Meaningful

Names used within the certificates shall identify the person or object to which assigned in a meaningful way. For equipment, this may be a model name and serial number, or an application

process (e.g., Organization X Mail Server). Any CA asserting this policy shall only sign certificates with subject names from within a name-space approved by the PMO and PMA.

The directory information tree must accurately reflect organizational structures. In addition, the common name shall represent the Subscriber in a way that is easily understandable for humans.

The common name within the DN must respect name space uniqueness requirements and must not be misleading. This does not preclude the use of pseudonymous certificates as defined in Section 3.1.3.

While the issuer name in CA certificates is not generally interpreted by relying parties, this CP requires use of meaningful names by CAs issuing under this policy. If included, the common name should describe the issuer, such as:

cn=*Treasury Operational CA-1*

The subject name in CA certificates must match the issuer name in certificates issued by the subject, as required by RFC 3280.

3.1.3 Anonymity or Pseudonymity of Subscribers

The TRCA shall not issue anonymous certificates. Subordinate CAs may issue pseudonymous certificates to support internal operations. CA certificates issued by the TRCA shall not contain anonymous or pseudonymous identities.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting name forms will use the appropriate standard. Rules for interpreting distinguished name forms are specified in X.501. Rules for interpreting e-mail addresses are specified in [RFC 2822]. Rules for interpreting the pivFASC-N name type are specified in [PACS].

3.1.5 Uniqueness of Names

The Treasury CMAs must enforce name uniqueness within the X.500 name space, which they have been authorized, and that uniqueness shall be enforced by the PMO under the auspices of the Treasury Office of the CIO. The userID attribute is used to ensure that no two individuals are assigned the same DN, and therefore potentially the same electronic identity or credential.

Each DoT PKI CA will unambiguously identify each object in the naming hierarchy for the certificate repository using DNs. The DoT CAs will ensure that a DN, once assigned, remains unique for the lifetime of the PKI, and will not re-use that name to identify a different entity.

When other name forms are used, CMAs must allocate them, to ensure such name uniqueness across the Department. Each DoT PKI CA shall document in its CPS;

- What name forms shall be used,

- How the TCA will interact with the enterprise services to ensure this is accomplished, and
- How Treasury will allocate names within the Subscriber community to guarantee name uniqueness among current and past Subscribers (e.g., if "Joe Smith" leaves a CA's community of Subscribers, and a new, different "Joe Smith" enters the same community of Subscribers, how will these two people be provided unique names?).

The CMA shall investigate and if necessary recommend the correction for any name collisions brought to its attention. The CMA shall coordinate with and defer to the PMO where appropriate.

3.1.6 Recognition, Authentication, & Role of Trademarks

The CMA shall investigate and if necessary recommend the correction for any trademark name collisions brought to its attention. The CMA shall coordinate with and defer to the PMO where appropriate. The CMA will communicate resolutions to all interested parties. Consistent with Federal Policy, DoT PKI CAs will not knowingly use trademarks in names unless the subject has the rights to use that name.

3.2 INITIAL IDENTITY VALIDATION

Certificate applicants must communicate application requests for certificates to an authorized RA or LRA via a trustworthy process, but generally in person. An authorized RA, equipped with Registration Authority hardware and software, may communicate authorizations to issue Certificates directly to the supporting CA electronically, provided all communication is secure. An LRA, who is not equipped with Registration Authority hardware and software, must transmit authorization requests to issue Certificates to the appropriate RA by secure means (i.e., digitally signed electronic means, via registered mail, or in person).

3.2.1 Method to Prove Possession of Private Key

In the case where the CMA generates the key directly on the Subscriber's token, or in a key generator that benignly transfers the key to the Subscriber's token, then the end-entity is presumed to be in possession of the private key at the time of generation or transfer and proof of possession is not required. If the user is not in possession of the token during key generation, the CMA shall deliver the token to the Subscriber via an accountable method (see Section 6.1.2). The CMA must obtain acknowledgment of receipt from the Subscriber of shipment or must revoke any certificates issued to that Subscriber. The CMA must deliver activation data for the private keys within the token or module to the Subscriber through a separate, secure communication unless the CMA delivers the token or module in person.

When the CMA delivers keyed hardware tokens to Subscribers, they must accomplish delivery in a way that ensures that they provide the correct tokens and activation data to the correct people. The CMA shall maintain a Subscriber token receipt validation record. When any mechanism that includes a shared secret (e.g., a password or PIN) is used, the mechanism shall ensure that the applicant and the CMA are the only recipients of this shared secret.

In those cases where the Subscriber causes the system to generate keys (e.g., remote emergency renewal), the Subscriber is required to prove possession of the private key that corresponds to the public key in the certificate request to the CMA.

3.2.2 Authentication of Organization Identity

A DoT PKI CA may issue certificates directly in the name of an organization rather than an individual for those functions and applications performed on behalf of the organization. The CMA must authenticate the identity of any organization that appears as a component of a subject name appearing in a certificate issued by the CA before processing the certificate application. Any organization requesting a certificate must have a PKI Sponsor to accept the obligations of the organization. This section pertains only to the authentication and naming of an organization as the subject in a certificate.

Requests for certificates in the name of an organization or group shall include the necessary identifying data of the Sponsor, the group or organization name, address, and documentation of the existence of the organization. This information will include but is not limited to the following:

- Organization identification and authorization
- Contact information to enable the CMA to communicate with the PKI Sponsor as required

The CMA shall verify this information, in addition to the authenticity and authorization of the requesting PKI Sponsor, authenticate the validity of any authorizations to be asserted in the certificate, and verify the source and integrity of the data collected to an assurance level commensurate with the certificate assurance level requested. The CPS will specify acceptable measures for authenticating both the organization and PKI Sponsor's identity and authorizations.

The CMA shall also include his or her own identity information and authentication declaration as outlined in Section 3.2.3. The PKI Sponsor shall present information sufficient for registration at the level of assurance requested, for both himself or herself and the non-human Entity (i.e., organization or group) requesting a certificate, and shall authenticate this information in person as prescribed in Section 3.2.3.

3.2.3 Authentication of Individual Identity

3.2.3.1 Authentication of Human Subscribers

For Subscribers (including all RAs/LRAs and PKI Sponsors of organizations, components, and minors or others not legally competent), the CMA shall ensure that the applicant's identity information is verified in accordance with this CP, the applicable CPS, and all applicable MOAs. The CMA must ensure that the applicant's identity information and public key are adequately bound. For each assurance level, the applicant must meet the minimum set of requirements identified in this section. A CMA may use mechanisms of equivalent or stronger assurance if documented in their CPS. The appropriate DoT PKI CA CPS will specify the acceptable procedures for authenticating a Subscriber's identity.

The CMA must record the process followed for each certificate. Process information shall depend upon the certificate's level of assurance and shall be addressed in the applicable CPS. In addition, the documentation and authentication requirements shall vary depending upon the level of assurance. At a minimum, process documentation and authentication requirements must include the following, depending on the level of assurance for issuance of each certificate:

- Identity of the applicant
- Identity of the person performing the identification
- A signed declaration by that person that he or she verified the identity of the applicant against official government-issued photo ID as required using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law
- If in-person identity proofing is done, a unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s)
- The date of the verification
- A declaration of identity signed by the applicant using a handwritten signature and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law

For All Levels: As an alternative to presentation of identification credentials, the CMA may use other mechanisms of equivalent or greater assurance (such as comparison of biometric data to identities pre-verified to the standards of this policy, and obtained via authenticated interaction with secured databases).

For Medium and High Assurance: The CMA shall establish identity no more than 30 days before initial certificate issuance. Before enabling the applicant's certificate, the CMA shall personally verify the applicant's identity. Minors and others not legally competent to provide face-to-face registration information alone shall be accompanied by a person already certified by the PKI (i.e., a Sponsor), who will present information sufficient for registration at the level of the certificate being requested, for himself or herself, and the person accompanied. Persons not physically capable of providing face-to-face registration information shall be proxied by a person already certified by the PKI, who will present information sufficient for registration at the level of the certificate requested, for both himself or herself and the person unable to appear himself or herself.

For the Basic and Medium Assurance Levels: An Entity certified by a State or Federal Entity as being authorized to confirm identities may perform in-person authentication on behalf of the RA/LRA. The certified Entity forwards the information collected from the applicant directly to the RA/LRA in a secure manner. Packages secured in a tamper-evident manner by the certified Entity satisfy this requirement; other secure methods are also acceptable. Such authentication does not relieve the RA/LRA of responsibility to verify the presented data.

The table below summarizes the identification requirements for each level of assurance.

Table 3-2 Identification Requirements

Assurance Level	Identification Requirements
Rudimentary	No identification requirement; applicant may apply and receive a certificate by providing his or her e-mail address.
Basic	Applicant shall establish identity by in-person proofing before a RA/LRA, Trusted Agent, an Entity certified by a State or Federal Entity as being authorized to confirm identities; or remotely by providing verifying information including ID number and account number through record checks either with the applicable agency or institution, or through credit bureaus or similar databases. Such information confirms that: name, DoB, address, and other personal information in records are consistent with the application and sufficient to identify a unique individual[12]. RA/LRA shall confirm addresses by: a) Issuing credentials in a manner that confirms the address of record supplied by the applicant; or b) Issuing credentials in a manner that confirms the ability of the applicant to receive telephone communications at a number associated with the applicant in records, while recording the applicant's voice.
Medium (all policies)	Applicant shall establish identity by in-person proofing before the RA/LRA, Trusted Agent, or an Entity certified by a State or Federal Entity as being authorized to confirm identities; the proofing authority shall verify such information provided to ensure legitimacy. A trust relationship between the Trusted Agent and the applicant, based on an in-person antecedent, may suffice as meeting the in-person identity-proofing requirement. Credentials required are either one Federal Government-issued Picture I.D., or two non-Federal Government IDs, one of which shall be a photo I.D. (e.g., Drivers License).
High	Applicant shall establish identity by in-person appearance before the RA/LRA, or Trusted Agent; the proofing authority shall verify such information provided to ensure legitimacy Credentials required are either one Federal Government-issued Picture I.D., or two non-Federal Government IDs, one of which shall be a photo I.D. (e.g., Drivers License).

3.2.3.2 Authentication of Human Subscribers for Group Certificates

Normally, a CMA shall issue a certificate to a single Subscriber. For cases where there are several entities acting in one capacity, and where non-repudiation for transactions is not required, a certificate may be issued that corresponds to a private key that is shared by multiple Subscribers. Subordinate DoT PKI CAs and/or RA/LRAs shall record the information identified

[12] DoT PKI CMA shall not collect or retain personal information protected under the Privacy Act, but will rely upon such information collected and retained by the DoT PIV badging authority.

in Section 3.2.3.1 for a Sponsor from the organization's Information Systems Security Office or equivalent, as well as for the subordinate PKI CA CMA, before issuing a group certificate.

In addition to the authentication of the Sponsor, the RA/LRA shall perform the following procedures for members of the group:

- The Information Systems Security Office or equivalent shall be responsible for ensuring control of the private key, including maintaining a list of Subscribers who have access to use of the private key, and accounting for which Subscriber had control of the key at what time
- The subjectName DN must not imply that the subject is a single individual, e.g. by inclusion of a human name form
- The list of those holding the shared private key must be provided to, and retained by, the applicable CA or its designated representative
- The procedures for issuing tokens for use in shared key applications must comply with all other stipulations of this CP (e.g., key generation, private key protection, and Subscriber obligations)

3.2.3.3 Authentication of Component Identities

Some computing and communications components (routers, firewalls, servers, etc.) will be named as certificate subjects. In such cases for all assurance levels, the component must have a human PKI Sponsor. The Sponsor is responsible for providing the CMA correct registration information regarding the end-entity as prescribed in the applicable DoT PKI CA CPS.

In the case of computing and communications components (equipment), this information shall include but is not limited to the following:

- Equipment or application organizational owner
- Equipment identification (e.g., serial number) or service name (e.g., DNS name)
- Equipment or application public keys
- Equipment or application authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the CA or RA to communicate with the Sponsor when required

The CMA shall authenticate the validity of any authorizations asserted in the certificate, and shall verify source and integrity of the data collected to an assurance level commensurate with the certificate assurance level requested. The CMA shall also include his or her own identity information and authentication declaration as outlined in Section 3.2.3.1. The PKI Sponsor will present information sufficient for registration at the level of assurance requested, for both himself or herself and the non-human Entity (e.g., equipment, groups) requesting a certificate, and shall authenticate this information in person as prescribed in Section 3.2.3.1.

Acceptable methods for performing this authentication and integrity checking include, but are not limited to the following:

- Verification of digitally signed messages sent from the Sponsor (using certificates of equivalent or greater assurance than that requested)
- In person registration by the Sponsor, with the identity of the Sponsor confirmed in accordance with the requirements of Section 3.2.3.1

3.2.4 Non-verified Subscriber Information

Except for the rudimentary assurance level, CMAs shall not include unverified information in certificates.

3.2.5 Validation of Authority

For cross certification, the DoT PKI OA shall validate the representative's authorization to act in the name of the organization, and include such verification in the recommendation to the PMA.

3.2.6 Criteria for Interoperation

The PMA shall determine the criteria for cross certification with other Entities in accordance with Section 1.1.5 and the U.S. Government Public Key Infrastructure Cross Certification Methodology and Criteria. (See http://www.cio.gov/fbca/documents.htm.)

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-key

Re-keying a certificate means that the CMA creates a new certificate that has the same characteristics and level as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key) and a different serial number and possibly different validity period.

In the event that a TRCA re-key is required, the FBCA will issue a new certificate to the TRCA. For any subordinate DoT PKI CA that requires a re-key, the TRCA will issue its new certificate. Before issuance, the subordinate CA shall identify itself through use of its current signature key or the initial registration process. If it has been more than three years since the subordinate CA identification as required in Section 3.2, the DoT PKI subordinate CA shall re-establish identity through the initial registration process.

Subscribers must periodically obtain new keys and re-establish identity as defined in Section 3.2. A DoT PKI CA may re-key Subscribers based on electronically authenticated Subscriber requests. Subscribers must stop using private keys before the public key expires. Confidentiality private keys do not have a lifetime so Subscribers may use these keys at any time to decrypt information.

The following key lifetimes given are maximums. A program may always require shorter lifetimes. The following key lifetimes are for end entities, Section 5.6 provides TRCA key lifetimes:

Table 3-3 End Entities Certificate Life Times

Assurance Level	Public Key Certificate Lifetimes
Rudimentary	Signature & confidentiality keys re-key every five years
Basic	Signature & confidentiality keys re-key every five years
Medium (all policies)	Signature & confidentiality keys re-key every three years
High	Signature & confidentiality keys re-key every three years

Subscribers of DoT PKI CAs shall identify themselves for the purpose of re-keying as required below:

Table 3-4 Subscriber Routine Re-key Identity Requirements

Assurance Level	Routine Re-key Identity Requirements for Subscriber Signature and Encryption Certificates
Rudimentary	Subscriber may establish identity through use of current signature key.
Basic	Subscriber may establish identity through use of current signature key, except that the Subscriber shall re-establish identity through initial registration process at least once every fifteen years from the time of initial registration.
Medium (all policies)	Subscriber may establish identity through use of current signature key, except that the Subscriber shall re-establish identity through initial registration process at least once every nine years from the time of initial registration, or as required by renewal of PIV Card.
High	Subscriber may establish identity through use of current signature key, except that identity shall be established through initial registration process at least once every three years from the time of initial registration, or as required by renewal of PIV Card.

If DoT implements the capability of associating authorizations with a certificate, including any conveyed or implied by the subject's DN, the Subscriber and/or the Subscriber's organization shall notify the appropriate CAs of the withdrawal of authorization. The CPS shall document the mechanisms used to notify the appropriate CAs of this action. In such instances, withdrawal of authorization may result in revocation of the old certificate and, if necessary, the issuance of a new certificate with a different public key and the appropriate associated authorizations.

3.3.1.1 Certificate Renewal

Renewing a certificate means creating a new certificate with the same name, key, and authorizations as the old one, but a new, extended validity period, and a new serial number. The DoT PKI Treasury TRCA shall not perform certificate renewal. Any certificate issued by a TRCA with a new serial number must contain a unique public key not previously certified. Subordinate PKI CAs may renew certificates. A DoT PKI CA may renew a certificate if the public key has not reached the end of its validity, the associated private key has not been compromised, and the user name and attributes are still correct. The PKI CA need not revoke the old certificate, but may not re-key, renew, or update it further. See Section 4.6.

3.3.1.2 Certificate Update

Updating a certificate means creating a new certificate that has the same or a different key, a different serial number, and differs in one or more other fields, from the old certificate. The TRCA shall not create a new certificate containing a public key that exists in another certificate. DoT PKI subordinate CAs may or may not revoke the old certificate[13], but must not re-key, renew, or update it further. Except at Rudimentary assurance, if a Subscriber's common name is legally changed (e.g., due to marriage or divorce), then legal proof of the name change (i.e., the same requirements used to apply for a certificate) must be provided to the Designated Naming Authority to initiate the name change process in the directory structure. Once this change has taken place, the individual must appear before (or be validated by) an RA/LRA in order for an updated certificate having the new name to be issued.

When a DoT PKI CA updates its private signature key and thus generates a new public key, the DoT PKI CA shall notify all CAs, RAs, and Subscribers that rely on the CA's certificate of the change. For self-signed (i.e., TRCA) certificates, such certificates shall be conveyed to users in a secure fashion to preclude malicious substitution attacks.

3.3.2 Identification and Authentication for Re-key after Revocation

For all levels of assurance, Subscribers requesting certificates after revocation, other than during a renewal or update action, must meet initial identity authentication and registration requirements, as indicated in Section 3.2 to obtain a new certificate. (This applies to all certificates issued by both a TRCA and any subordinate DoT PKI CA.)

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

The CMA must authenticate revocation requests in accordance with Section 4.9.3. The CMA may authenticate requests to revoke a certificate using signatures generated with that certificate's associated private key, regardless of whether or not the private key has been compromised.

[13] PIV Card Authentication certificates must be revoked upon issuance of a new PIV credential. Digital signature key histories and encryption certificates shall be recovered and transferred in accordance with the applicable PKI CA CPS and the Department of the Treasury Key Recovery Policy (KRP) and Key Recovery Practices Statement (KRPS).

4. CERTIFICATE LIFE-CYCLE

4.1 APPLICATION

This policy identifies the minimum requirements and procedures that are necessary to support trust in the PKI, without imposing specific implementation requirements on CMAs or users, and specifies requirements for initial application for certificate issuance.

The TRCA shall issue end-entity certificates to trusted role PKI Program Team personnel where necessary for the internal operations of the PKI TRCA. The TRCA will not issue end-entity certificates for any other reasons.

4.1.1 Submission of Certificate Application

For the TRCA, the DoT PMA shall submit the certificate application to the FPKIPA. For subordinate DoT PKI CAs, subordinate and/or supported activities shall submit requests for subordinate PKI CA certificates to the Department of the Treasury PKI PMO using the contact information provided in Section 1.5.2. Subscriber applicants shall follow the procedures in Section 4.2 of this CP and the applicable CPS.

4.1.2 Enrollment Process and Responsibilities

Within the Department, only the TRCA shall apply for cross certification with the FBCA, using the procedures outlined in the FBCA CP, the U.S. Government Public Key Infrastructure Cross Certification Criteria and Methodology with the U.S. Federal Bridge Certification Authority (FBCA) or Citizen and Commerce Class Common Certification Authority (C4CA) (http://www.cio.gov/fbca/documents.htm), and the MOA.

Only the TRCA shall cross certify with external CAs, or establish subordinate CAs. A Certification Practices Statement, written to the format of the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647) shall accompany all such requests.

Entities applying for cross certification are responsible for providing accurate information on their certificate applications. Upon issuance, the CMA shall manually check each certificate issued to a CA by the TRCA to ensure the proper population of each field and extension with the correct information before delivering the certificate to the Entity.

All CMAs shall conform to the CPS as written for the applicable CA. All CMAs shall authenticate, and protect from modification, communications among PKI authorities supporting the certificate application and issuance process.

4.2 CERTIFICATE APPLICATION PROCESSING

The CMA shall verify the accuracy of certificate application information, using procedures as specified in the applicable CPS, before issuing certificates.

4.2.1 Performing Identification and Authentication Functions

For the TRCA, the DoT PKI PMA shall validate acceptance of applicant identification and authentication.

For subordinate DoT PKI CAs, the identification and authentication of the Subscriber must meet the requirements specified for Subscriber authentication as specified in Sections 3.2 and 3.3. The applicant and the supporting CMA must perform the steps outlined in the applicable CPS when an applicant applies for a certificate. The CMA and Subscribers may perform these steps in any order that is convenient and that does not defeat security; however, they must complete all steps before certificate issuance.

CMAs shall authenticate and protect from modification all communications supporting the certificate application and issuance process using mechanisms commensurate with the protection requirements of the data. CMAs shall protect from unauthorized disclosure any electronic transmission of this data (i.e., encryption) commensurate with the protection requirements of the data.

4.2.2 Approval or Rejection of Certificate Applications

The PMA shall require an initial compliance audit to ensure that the DoT PKI CAs and other Entity CAs are prepared to implement all aspects of the applicable CPS, before authorizing the DoT PKI PMO to issue and manage certificates asserting Department of the Treasury certificate policies. DoT PKI CAs shall only issue certificates asserting Department of the Treasury certificate policies upon receipt of written notification from the DoT PMA authorizing them to do so.

The DoT PKI PMO and RAs/LRAs may reject any Subscriber, group, or component application that is incomplete, or that contains information that they cannot verify as accurate in accordance with Section 4.2.1. The CMA may afford Subscribers and Sponsors the opportunity to complete and/or augment application information. Failure to do so will result in denial of PKI certificates; and the CMA shall submit a report via protected communications to the DoT PKI PMO, outlining the circumstances and providing full identifying data about the applicant (i.e., Subscriber, organization, or device) and any Sponsor.

4.2.3 Time to Process Certificate Applications

CMAs shall identify and authenticate Subscribers, organizations, components, and PKI Sponsors not more than 30 days prior to certificate issuance. Otherwise, the CMA must re-confirm the identity to ensure issuance of the certificates to the appropriate individual.

4.3 ISSUANCE

4.3.1 CA Actions during Certificate Issuance

It is the responsibility of the CMA to verify that the certificate information is correct and accurate. The CMA shall check all CA certificates to ensure that all fields and extensions are properly populated. The CMA shall not sign any certificate until the RA and/or LRA have

completed all verifications and modifications, if any, to the CA's satisfaction, and the identification and authentication process set forth in the CP and appropriate CPS are complete. If an RA or LRA denies a certificate request, then the CA shall not sign the requested certificate.

CMAs shall verify all authorization and other attribute information received from an applicant. In most cases, the RA or LRA is responsible for verifying applicant data, but if CAs accept applicant data directly from applicants, then the CA is responsible for verifying the applicant data. The CMA shall verify information regarding attributes via those offices or roles that have authority to assign the information or attribute. The applicable CPS describes these processes and relationships.

4.3.2 Notification to Subscriber of Certificate Issuance

Where notification is not an integral component of the issuance process (e.g., when individual is present as the certificate is generated on their token), DoT PKI CAs shall proactively notify Subscribers that certificates have been generated.

4.4 ACCEPTANCE

Before a Subscriber can make effective use of the private key, the CMA shall convey their responsibilities to the Subscriber (or Sponsor in the case of group/organization or device certificates) as defined in Section 9.6.

For Rudimentary assurance, there is no stipulation. For all other assurance levels before a CA provides a Subscriber or Sponsor with the private key and allows its effective use, a CMA shall inform the Subscriber of the certificate's contents and responsibilities for its use and security; and require and document the Subscriber's acceptance of those obligations. The CPS outlines the specific steps for conveying responsibilities.

4.4.1 Conduct constituting certificate acceptance

Failure to object to the certificate or its contents constitutes acceptance of the certificate.

4.4.2 Publication of the Certificate by the CA

As specified in 2.2.1, each DoT PKI CA shall publish all CA and Subscriber certificates in the appropriate certificate repositories.

4.4.3 Notification of Certificate Issuance by the CA to other entities

For the TRCA, the DoT PKI PMA shall provide notification to all subordinate and cross certified entities, including the FPKIPA upon issuance of new inter-organizational CA cross certificates.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

For High, Medium Hardware, Medium, and Basic Assurance, Subscribers shall protect their private keys from access by other parties. For Rudimentary assurance, this CP makes no stipulation. Section 1.4 outlines authorized and prohibited uses of PKI certificates.

The DoT PKI CA shall specify restrictions in the intended scope of usage for a private key through certificate extensions, including the key usage and other extensions as needed, in the associated certificate.

4.5.2 Relying Party Public key and Certificate Usage

TRCA certificates, issued to subordinate and cross certified CAs, shall specify restrictions on use through critical certificate extensions, including the key usage extensions. Basic constraints may also appear if set to critical in accordance with the FPKI-PROF. DoT PKI CAs shall issue CRLs specifying the status of all unexpired certificates. Relying parties should process and comply with this information whenever using DoT PKI CA-issued certificates in a transaction.

4.6 Certificate Renewal

Certificate renewal consists of issuing a new certificate with a new validity period and serial number while retaining all other information in the original certificate including the public key. Frequent renewal of certificates may assist in reducing the size of CRLs. The TRCA shall not perform certificate renewal for CA or Subscriber certificates.

Where permitted after certificate renewal, a DoT PKI CA may or may not revoke the old certificate, but must not re-key, renew, or modify it further.

4.6.1 Circumstance for Certificate Renewal

Subordinate DoT PKI CAs may renew Subscriber certificates if the public key has not reached the end of its validity period, the associated private key has not been compromised or expired, and the Subscriber name and attributes are unchanged. In addition, the validity period of the certificate must meet the requirements specified in Section 6.3.2. DoT PKI CAs may also renew Subscriber certificates when the CA re-keys. The CMA may renew OCSP Responder certificates except that the aggregated lifetime of the public key shall not exceed the certificate lifetime specified in Section 6.3.2.

4.6.2 Who may Request Renewal

For subordinate DoT PKI CAs that support renewal, the CA shall only accept renewal requests from certificate Subscribers, PKI Sponsors, or RAs. Additionally, a DoT PKI CA may perform renewal of its Subscriber certificates without a corresponding request, such as when the CA re-keys.

4.6.3 Processing Certificate Renewal Requests

For DoT PKI CAs that support renewal, the DoT PKI PMO shall approve certificate renewal for reasons other than re-key of the PKI CA.

4.6.4 Notification of new certificate issuance to Subscriber

Subordinate DoT PKI CAs shall proactively notify affected Subscribers of certificate renewal by any appropriate and secure means.

4.6.5 Conduct constituting acceptance of a Renewal certificate

Failure to object to the certificate or its contents constitutes acceptance of the certificate.

4.6.6 Publication of the Renewal certificate by the CA

As specified in Section 2.2.1, each DoT PKI CA shall publish all CA and Subscriber certificates in the appropriate certificate repositories.

4.6.7 Notification of Certificate Issuance by the CA to other entities

For subordinate DoT PKI CAs, the responsible Operating Authority shall notify the DoT PKI PMO.

4.7 CERTIFICATE RE-KEY

Re-keying a certificate consists of creating new certificates with a different public key (and serial number) while retaining the remaining contents of the old certificate that describe the subject. The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key. After certificate re-key, the CA may or may not revoke the old certificate, but must not re-key, renew, or modify it further.

Subscribers of Entity CAs shall identify themselves for the purpose of re-keying as required in Section 3.3.

4.7.1 Circumstance for Certificate Re-key

The TRCA will issue new cross certificates to subordinate or cross certified CAs when a currently recognized subordinate or cross certified CA has generated a new key pair and a valid CPS exists between the TRCA and the subordinate or cross certified CAs.

4.7.2 Who may request certification of a new public key

The DoT PKI PMA may request certification of a new public key for subordinate DoT PKI CAs or cross certified Entity Principal CAs. For subordinate CAs that support re-key, the CA shall only accept such requests from the subject of the certificate or PKI Sponsors. Additionally, CAs and RAs may initiate re-key of a Subscriber's certificates without a corresponding request.

4.7.3 Processing certificate Re-keying requests

For TRCA, before performing re-keys on cross-certified or subordinate CAs, the DoT PKI PMA shall identify and authenticate Principal CAs by performing the identification processes defined in Section 3.2 or 3.3. The validity period associated with the new certificate must not extend beyond the period of the MOA.

For subordinate CAs, see Sections 3.2 and 3.3.

4.7.4 Notification of new certificate issuance to Subscriber

The DoT PKI PMO shall notify subordinate DoT PKI CAs and cross certified Entity Principal CAs upon issuance of new certificates. Subordinate CAs shall proactively notify affected Subscribers of certificate renewal by any appropriate and secure means.

4.7.5 Conduct constituting acceptance of a Re-keyed certificate

Failure to object to the certificate or its contents constitutes acceptance of the certificate.

4.7.6 Publication of the Re-keyed certificate by the CA

As specified in Section 2.2.1, each DoT PKI CA shall publish all CA and Subscriber certificates in the appropriate certificate repositories.

4.7.7 Notification of certificate issuance by the CA to other Entities

For the TRCA, the DoT PKI PMA shall provide notification to all subordinate and cross certified entities, including the FPKIPA upon issuance of renewed inter-organizational CA cross certificates. For subordinate CAs, the responsible Operating Authority shall notify the DoT PKI PMO.

4.8 MODIFICATION

Certificate modification (a.k.a. update) consists of creating new certificates with subject information (e.g., a name or email address) that differs from the old certificate. For example, a subordinate DoT PKI CA may perform certificate modification for a Subscriber whose characteristics have changed (e.g., has just received a medical degree). The new certificate may not have the same or different subject public key.

After certificate modification, the DoT PKI CA may or may not revoke the old certificate, but must not re-key, renew, or modify it further.

4.8.1 Circumstance for Certificate Modification

For the TRCA, the CA performs certificate modification if the subordinate DoT PKI CA or cross certified Entity CA changes its name. For subordinate CAs and cross certified Entity CAs, the CA performs certificate modification if the subject changes their name or other identifying data included in the certificate.

4.8.2 Who may request Certificate Modification

The DoT PKI PMO or the subordinate CA (or cross certified Principal CA) PKI OA may request certificate modification for subordinate DoT PKI CAs (or cross certified Entity Principal CAs).

For subordinate DoT PKI CAs that support modification, the CA shall only accept such requests from the subject of the certificate or PKI Sponsors. CAs and RAs may initiate modification of a Subscriber's certificates without a corresponding request in cases where the change is the result of a modification to the CA or the directory.

4.8.3 Processing Certificate Modification Requests

For the TRCA, the DoT PKI OA shall perform certificate modification at the direction of the PMA. The PKI OA may also perform certificate modification at the request of a subordinate or cross certified CA for the following reasons:

- Modification of SIA extension
- Minor name changes (e.g., change XXCA to XXCA1) as part of key rollover procedures

The validity period associated with the new certificate must not extend beyond the period of the MOA and the Security Officer must verify the information before the CA issues the modified certificate.

For subordinate DoT PKI CAs, the Subscriber must provide proof of all Subscriber information changes to the RA/LRA or other designated agent; and the RA/LRA must verify the information before the CA issues the modified certificate.

4.8.4 Notification of new certificate issuance to Subscriber

The DoT PKI PMA shall notify subordinate DoT PKI CAs and cross certified Entity Principal CAs upon issuance of new certificates. Subordinate DoT PKI CAs shall proactively notify affected Subscribers of certificate renewal or modification by any appropriate and secure means.

4.8.5 Conduct constituting acceptance of modified certificate

Failure to object to the certificate or its contents constitutes acceptance of the certificate.

4.8.6 Publication of the modified certificate by the CA

As specified in Section 2.2.1, each DoT PKI CA shall publish all CA and Subscriber certificates in the appropriate certificate repositories.

4.8.7 Notification of certificate issuance by the CA to other Entities

For the TRCA, the DoT PKI PMA shall provide notification to all subordinate and cross certified entities, including the FPKIPA upon issuance of modified inter-organizational CA cross certificates. For subordinate DoT PKI CAs, the responsible Operating Authority shall notify the DoT PKI PMO.

4.9 CERTIFICATE REVOCATION & SUSPENSION

The CMA must authenticate all revocation requests. CMAs may authenticate requests to revoke a certificate using that certificate's associated private key, regardless of whether or not the private key has been compromised. For High, Medium Hardware, Medium, and Basic Assurance, all CAs shall publish CRLs.

4.9.1 Circumstances for Revocation

The CMA will revoke certificates issued by the TRCA under three circumstances:

- The first circumstance is when the PMA requests revocation of a TRCA-issued certificate. This will be the normal mechanism for revocation in cases where the PMA determines that a subordinate DoT PKI CA or a cross certified Entity PKI does not meet the DoT PKI CP requirements or certification of the Entity PKI is no longer in the best interests of the Department of the Treasury or the Federal Government.
- The second circumstance is when the DoT PKI PMO receives an authenticated request from a previously designated official of the cross certified Entity responsible for the Principal CA.
- The third circumstance is when the DoT PKI Program Team determines that an emergency has occurred that may affect the integrity of the certificates issued by a DoT PKI CA. Under such circumstances, the following individuals may authorize immediate certificate revocation:
  - DoT PMA
  - DoT PKI PMO
  - DoT PKI OA

The PMA shall review the emergency revocation as soon as practicable. The TRCA shall revoke, at a minimum, certificates for the reason of key compromise upon receipt of an authenticated request from a subordinate DoT PKI CA or cross certified Entity. Whenever any of the above circumstances occur, the TRCA shall revoke the associated certificate and place it on the appropriate revocation list. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.

For the TRCA, subordinate DoT PKI CAs, and cross certified Entity CAs, the CMA shall revoke a certificate when the binding between the subject and the subject's public key defined within a certificate, excluding DN changes, is no longer considered valid.

The CMA shall revoke a Subscriber certificate when the binding between the subject and the subject's public key defined within a certificate is no longer valid. Examples of circumstances that invalidate the binding are:

- The Subscriber can be shown to have violated the stipulations of its Subscriber obligations and/or agreement
- The private key is suspected of compromise

- The user or other authorized party (as defined in the CPS) makes a formal request to the CMA asking to revoke his or her certificate
- Privileged attributes if implemented, asserted in the Subscriber's certificate are reduced

Whenever any of the above circumstances occur, the CMA revokes the associated certificate and places it on the CRL. Once revoked, a certificate will remain on the CRL or ARL at least until the certificate expires.

4.9.2 Who Can Request Revocation

The PMA may direct revocation of a TRCA certificate, or certificate issued by the TRCA. Subordinate DoT PKI CAs and cross certified Entity CAs shall accept, at a minimum, revocation requests from Subscribers. The CMA may support requests for certificate revocation from other parties as specified in the appropriate CPS. A cross certified Entity Principal CA may always revoke the certificate it has issued to a TRCA without PMA action.

Within the TCA, a CA may summarily revoke certificates within its domain. An RA may request the revocation of a Subscriber's certificate on behalf of any authorized party as specified in its CPS or Subscriber agreements. A Subscriber can request the revocation of his or her own certificate(s).

4.9.3 Procedure for Revocation Request

Upon receipt of a revocation request involving a TRCA-issued certificate, the DoT PKI OA shall authenticate the request and apprise the PMO and PMA. The PMA may take whatever measures it deems appropriate to verify the need for revocation. If the revocation request appears valid, the PMA shall direct the DoT PKI OA to revoke the certificate. The DoT PKI OA shall give prompt oral or electronic notification to previously designated officials in all subordinate DoT PKI CAs and cross certified Entities having a Principal CA with which the TRCA interoperates.

Subordinate DoT PKI CAs and cross certified Entity CAs that implement certificate revocation shall revoke certificates upon receipt of sufficient evidence of compromise or loss of the Subscriber's corresponding private key. A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and provide a means for the request to be authenticated (e.g., digitally, or manually signed). Where Subscribers use hardware tokens, revocation is optional if all the following conditions are met:

- the revocation request was not for key compromise;
- the hardware token does not permit the Subscriber to export the signature private key;
- the Subscriber surrendered the token to the PKI CMA;
- the token was zeroized or destroyed promptly upon surrender;
- the token has been protected from malicious use between surrender and zeroization or destruction.

In all other cases, revocation of the certificates is mandatory. Even where all the above conditions have been met, revocation of the associated certificates is recommended.

Upon receipt of a revocation request from the Subscriber or another authorized party, the CA shall authenticate the revocation request. At its discretion, the CA may take reasonable measures to verify the need for revocation. Revocation takes effect upon publication of status information.

For PKI implementations using hardware tokens, Subscribers leaving organizations that sponsored their participation in the PKI shall surrender to their CMA (through any accountable mechanism) all cryptographic hardware tokens issued under the sponsoring organization before leaving the organization. If the CA cannot obtain the hardware tokens when a Subscriber leaves an organization, then the CA, immediately upon notification, shall revoke all Subscribers' certificates associated with the un-retrieved tokens with the reason specified as key compromise. If later recovered, the token shall be zeroized or destroyed promptly upon surrender and shall be protected from malicious use between surrender and being zeroized or destroyed.

4.9.4 Revocation Request Grace Period

There is no grace period for revocation under this policy; the Subscribers and authorized parties must notify the CMA as soon as they identify the need to revoke a certificate. CAs will revoke certificates as quickly as practical upon receipt of a proper revocation request, and shall always revoke certificates within the time constraints described in Section 4.9.5. See also Section 9.6.3.

4.9.5 Time within which CA must Process the Revocation Request

The TRCA and subordinate CAs will revoke certificates as quickly as practical upon receipt of a proper revocation request. Revocation requests shall be processed before the next CRL is published, excepting those requests validated within two hours of CRL issuance. Revocation requests validated within two hours of CRL issuance shall be processed before the following CRL is published. A request is considered received when a Trusted Role authorized to revoke certificates, first accesses a valid request.

4.9.6 Revocation Checking Requirements for Relying Parties

This CP makes no stipulation. Use of revoked certificates could have damaging or catastrophic consequences. The Relying Party and/or System Accreditor make any determinations on the matter of how often new revocation data should be obtained, considering the risk, responsibility, and consequences for using a certificate whose revocation status cannot be guaranteed.

4.9.7 CRL Issuance Frequency

For this CP, issuance encompasses both ARL and CRL generation and publication. To the extent practical, the CMA shall check the contents of ARLs and CRLs before issuance to ensure that all information is correct

To ensure timeliness of information, every CA shall periodically issue and post a CRL to a repository, even if there are no changes or updates required. A CA may issue CRLs more

frequently than required. DoT PKI CAs shall post an early update to an applicable Revocation List in the event of a revocation due to key compromise. All CRLs shall populate nextUpdate field. CAs that issue certificates to subscribers or operate online must issue CRLs at least once every 18 hours, and the *nextUpdate* time in the CRL may be no later than 18 hours after issuance time (i.e. the *thisUpdate* time). This will facilitate the local caching of certificate status information for offline or remote (laptop) operation.

CAs shall make public a description of how to obtain revocation information for the certificates they issue, and an explanation of the consequences of using dated revocation information. This information shall be given to subscribers during certificate request or issuance, and shall be readily available to any potential relying party.

For each assurance level, the minimum issuance frequencies for routine CRLs are as follows:

Table 4-1 CRL Issuance Frequency

Assurance Level	Maximum Interval for Routine CRL Issuance	Maximum Interval for Emergency CRL Issuance
Rudimentary	No stipulation	No stipulation
Basic	18 hours	18 hours after notification
Medium (all policies)	18 hours	18 hours after notification
High	18 hours	Six hours after notification

For CAs that only issue CA certificates and are operated in an off-line manner, routine CRLs may be issued less frequently than specified above. However, the interval between routine CRL issuance shall not exceed 31 days. Such CAs must meet the requirements specified above for issuing Emergency CRLs. (Note: Such CAs will also be required to notify the FPKI Operational Authority upon Emergency CRL issuance.)

4.9.8 Maximum Latency of CRLs

DoT PKI CAs shall publish CRLs within four hours of generation. (See Section 4.9.7) The CAs shall publish each CRL no later than the time specified in the *nextUpdate* field of the previously issued CRL for same scope.

4.9.9 On-line Revocation/Status Checking Availability

CAs and Relying Party client applications may optionally support online status checking. Since the Department of the Treasury operates in some environments that cannot accommodate online communications, all DoT PKI CAs shall be required to support CRLs.

Online Certificate Status Authority (OCSA) used for verifying certificates asserting Department of the Treasury certificate policies shall perform the following actions:

- Certificates indicated as being valid have a chain of valid certificates (valid as defined by X.509) linking back to the TRCA
- Each certificate in the certificate chain used to validate the certificate whose status is being requested is checked for revocation, such that the Relying Party need not check more than one CSA to validate a Subscriber certificate
- The certificate status response makes clear which attributes, if any and if used, other than certificate subject name the CSA authenticates

If an Entity CA supports on-line revocation/status checking, the latency of certificate status information distributed on-line by Entity CAs or their delegated status responders must meet or exceed the requirements for CRL issuance stated in Section 4.9.7.

4.9.10 On-line Revocation Checking Requirements

This CP makes no stipulation. Clients using online revocation checking need not obtain or process CRLs, at their own discretion.

4.9.11 Other Forms of Revocation Advertisements Available

A CA may also use other methods to publicize the certificates it has revoked. Any alternative method must meet the following requirements:

- The alternative method must be described in the appropriate CPS.
- The alternative method must provide authentication and integrity services commensurate with the assurance level of the certificate being verified.
- Any alternate forms used to disseminate revocation information shall be implemented in a manner consistent with the security and latency requirements for the implementation of CRLs and online revocation and status checking in Sections 4.9.5, 4.9.7, 4.9.8, and 4.9.9.

4.9.12 Special Requirements Related To Key Compromise

In the event of a TRCA or Entity Principal CA private key compromise or loss, the cross certificates shall be revoked and a CRL shall be published at the earliest feasible time by the DoT PKI OA.

For subordinate DoT PKI CAs, when a CA certificate is revoked or Subscriber certificate is revoked because of compromise, or suspected compromise, of a private key, a CRL must be issued as specified below:

Table 4-2 Emergency CRL Issuance Frequency

Assurance Level	Maximum Latency for Emergency CRL Issuance
Rudimentary	No stipulation
Basic	24 hours after notification
Medium (all policies)	18 hours after notification
High	Six hours after notification

The CRL shall contain codes identifying the reason for revoking a certificate and/or specific key pair.

4.9.13 Circumstances for Suspension

This policy does not permit or recognize certificate suspension. Consequently, CAs may not consider certificates issued in contravention to this policy, and placed on a CRL, as valid.

4.9.14 Who can Request Suspension

This CP makes no further stipulation.

4.9.15 Procedure for Suspension Request

This CP makes no further stipulation.

4.9.16 Limits on Suspension Period

This CP makes no further stipulation.

4.10 CERTIFICATE STATUS SERVICES

This CP makes no further stipulation.

4.10.1 Operational Characteristics

This CP makes no further stipulation.

4.10.2 Service Availability

This CP makes no further stipulation.

4.10.3 Optional Features

This CP makes no further stipulation.

4.11 END OF SUBSCRIPTION

This CP makes no stipulation.

4.12 KEY ESCROW & RECOVERY

The TRCA shall not perform any encryption key recovery functions involving subordinate DoT PKI CAs or cross certified Entity CAs, and shall not store any information encrypted by the DoT PKI CA public key that may require key recovery capabilities. However, if and when encryption key pairs need to be issued by the TRCA covering repository system access or for other purposes, the PMA shall publish applicable requirements for that purpose.

4.12.1 Key Escrow and Recovery Policy and Practices

Department of the Treasury PKI key recovery policies and procedures are addressed in the Key Recovery Policy (KRP) and the Key Recovery Practices Statement (KRPS). The KRPS shall be identified in the CPS. DoT PKI CA private keys are never escrowed.

Subordinate DoT PKI CAs may escrow Subscriber key management keys to provide key recovery. The CA shall protect escrowed keys at no less than the level of security appropriate to the assurance level of the certificate.

Under no circumstances shall the DoT PKI CA or any third party hold in trust a Subscriber private signature key.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

TCA does not use session key encapsulation and recovery, and as such it is out of scope of this CP.

5. FACILITY MANAGEMENT & OPERATIONS CONTROLS

5.1 PHYSICAL CONTROLS

All DoT PKI CA equipment, including CA cryptographic modules, shall be protected from unauthorized access at all times. The TRCA shall impose physical security requirements that provide similar levels of protection as those specified below. All the physical control requirements apply equally to the DoT PKI Root and subordinate CAs.

5.1.1 Site Location & Construction

The location and construction of the facility housing DoT PKI CA equipment shall be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, shall provide robust protection against unauthorized access to CA equipment and records.

The location and construction of any facility housing CMA equipment and operations shall be in accordance with the Treasury Security Manual, TD P 15-71.

5.1.2 Physical Access

5.1.2.1 Physical Access for CA Equipment

The CMA staff and DoT PKI facilities shall protect DoT PKI CA equipment from unauthorized access at all times. The security mechanisms shall be commensurate with the level of threat in the equipment environment. Since the DoT PKI Treasury Root and subordinate CAs must plan to issue certificates at all levels of assurance, the DoT PKI OA shall operate and control all CAs on the presumption that each shall issue at least one High Assurance certificate.

The physical security requirements pertaining to DoT PKI CAs that issue Basic Assurance certificates are:

- Ensure no unauthorized access to the hardware is permitted
- Ensure all removable media and paper containing sensitive plain-text information is stored in secure containers

In addition to those requirements, the following requirements shall apply to DoT PKI CAs that issue Medium, Medium Hardware, or High assurance certificates:

- Ensure manual or electronic monitoring for unauthorized intrusion at all times
- Ensure an access log is maintained and inspected periodically
- Require two person physical access control to both the cryptographic module and computer system

Multiparty physical access control to CA equipment can be achieved by any combination of two or more trusted roles (see Section 5.2.2) as long as the tasks being conducted are segregated in accordance with the requirements and duties defined for each trusted role.

The CMAs shall inactivate removable CA cryptographic modules before storage. When not in use, the CMA staff shall place removable CMA cryptographic modules, removable media, and any activation information used to access or enable CMA cryptographic modules or CMA equipment, or paper containing sensitive plain-text information, in locked containers. Such containers shall be sufficient for housing equipment and information commensurate with the classification, sensitivity, or value of the information protected by the certificates issued by the CMA. CMA staff shall either memorize or record and store activation data in a manner commensurate with the security afforded the cryptographic module, and shall not store such data with the cryptographic module.

A security check of the facility housing DoT PKI CA equipment shall occur before leaving the facility unattended. At a minimum, the check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation
- Any security containers are properly secured
- Physical security systems are functioning properly
- The area is secured against unauthorized access

The DoT PKI OA shall explicitly designate a person or group of persons responsible for making such checks. When a group of persons is responsible, the DoT PKI OA shall maintain a log identifying the person performing a check in each instance. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.

The following requirements shall apply to CAs operating at the Medium or High assurance level:

- Be manually or electronically monitored for unauthorized intrusion at all times
- Ensure a visitor access log is maintained and periodically inspected

5.1.2.2 Physical Access for RA Equipment

RA and LRA equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. The RA and LRA shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated RA and LRA cryptographic tokens shall be protected against theft, loss, and unauthorized use. These security mechanisms shall be commensurate with the level of threat in the RA and LRA equipment environment.

5.1.2.3 Physical Access for CSS Equipment

Physical access control requirements for CSS equipment (if implemented) shall meet the DoT PKI CA physical access requirements specified in Section 5.1.2.1.

5.1.3 Power and Air Conditioning

The facility housing CA equipment shall have power and air conditioning sufficient to create a reliable operating environment. DoT PKI CAs operating at a Basic, Medium, or High assurance level shall have backup capability sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. In addition, the DoT PKI CA directories (containing TCA issued certificates and CRLs) shall have Uninterrupted Power sufficient for a minimum of six hours operation in the absence of commercial power. DoT PKI CAs shall employ appropriate mechanisms to ensure availability of repositories as specified in Section 2.2.1.

5.1.4 Water Exposures

This policy makes no stipulation on prevention of exposure of CA equipment to water beyond that called for by Treasury Security Manual, TD P 15-71 and best business practice. The PKI OA shall install CA equipment such that it is not in danger of exposure to water, and ensure installation of moisture detectors in areas susceptible to flooding. The requirement excludes potential water damage from fire prevention and protection measures (e.g., sprinkler systems). Contingency plans for a CA that has sprinklers for fire control shall address recovery if the sprinklers malfunction, or cause water damage outside the fire area.

5.1.5 Fire Prevention & Protection

This policy makes no stipulation on fire prevention and protection of CA equipment beyond that called for by Treasury Security Manual, TD P 15-71 and best business practice. A description of the CMA's approach for recovery from a fire disaster shall be included in the Disaster Recovery Plan required by Section 5.7.

5.1.6 Media Storage

Media shall be stored to protect it from accidental damage (water, fire, electromagnetic) and unauthorized access. Media that contains security audit, archive, or backup information shall be stored in a location separate from the CMA equipment.

5.1.7 Waste Disposal

CMAs shall remove or destroy normal office waste in accordance with local policy. The CMAs shall destroy media used to collect, transmit, or store sensitive information before disposal, such that the information is unrecoverable. Sensitive waste material (i.e., documentation) shall be disposed of in a secure fashion (e.g., shredding or burning).

5.1.8 Off-Site backup

For DoT PKI CAs operating at Basic, Medium, or High assurance levels full system backups, sufficient to recover from system failure, shall be made on a periodic schedule, as described in the respective CPS. Backups are to be performed and stored off-site not less than once per week. At least one full backup copy shall be stored at an offsite location (separate from the CA

equipment). Only the latest full backup need be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA.

5.2 PROCEDURAL CONTROLS

Unless stated otherwise, the requirements in this section apply equally to all DoT PKI CAs.

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible and above reproach or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust in the entire PKI. There are two approaches to increase the likelihood of successfully carrying out these roles. The first approach is to ensure that the person filling the role is trustworthy and properly trained. The second is to distribute the functions of the role among several people, so that any malicious activity requires collusion. Chapter 1 describes the requirements regarding design and configuration of the technology to avoid mistakes and counter inappropriate behavior.

The requirements of this policy are defined in terms of four roles. (Note: the information derives from the Certificate Issuing and Management Components (CIMC) Protection Profile.) Each CA shall maintain lists, including names, organizations, contact information, and copies of appointment memoranda of those who act in these trusted roles, and shall make them available during compliance audits. The CA will make this information a part of the permanent records of the CA. However, the CA shall not maintain personnel or investigative records requiring protection under the Privacy Act.

- Administrator – authorized to install, configure, and maintain the CA; establish and maintain Subscriber accounts; configure profiles and audit parameters; and generate component keys.
- Officer – authorized to request or approve certificates or certificate revocations.
- Auditor – authorized to maintain audit logs.
- Operator – authorized to perform system backup and recovery.

Section 5.2.4 identifies the roles required for each level of assurance.

The following subsections provide a detailed description of the responsibilities for each role:

5.2.1.1 Administrator

The Administrator role is responsible for the following:

- Installation, configuration, and maintenance of the CA
- Establishing and maintaining CA system accounts
- Configuring certificate profiles or templates and audit parameters
- Generating and backing up CA keys

Administrators do not issue certificates to Subscribers.

5.2.1.2 Officer

The Officer (a.k.a. Security Officer, Registration Authority) role is responsible for issuing certificates, that is:

- Registering new Subscribers and securely requesting the issuance of certificates
- Verifying the identity of Subscribers, validity of documentation, and accuracy of information included in certificates
- Approving and executing the issuance of certificates
- Requesting, approving and executing the revocation of certificates
- Receiving, controlling, and distributing Subscriber certificates on FIPS 140 Level 2 compliant hardware tokens (cryptographic modules containing the CA private key), as specified in this CP and the applicable DoT CPS

The Officer also performs the administration and operation of the RA workstation.

5.2.1.3 Auditor

The Auditor role is responsible for the following:

- Reviewing, maintaining, and archiving audit logs
- Performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with its CPS

5.2.1.4 Operator

The Operator role is responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media.

5.2.2 Number of Persons Required per Task

Only one person is required per task for CAs operating at the Rudimentary and Basic Levels of Assurance. Medium, Medium Hardware, and High assurance CAs shall enforce multi-person controls on the CA private signing key to prevent duplication or theft without collusion.

Two or more persons are required for CAs operating at the Medium, Medium Hardware, or High Levels of Assurance for the following tasks only:

- CA key generation
- CA signing key activation
- CA private key backup

Where multiparty control for logical access is required, at least one of the participants shall be an Administrator. All participants must serve in a trusted role as defined in Section 5.2.1.

Multiparty control for logical access shall not be achieved using personnel that serve in the Auditor Trusted Role.

Physical access to the CAs does not constitute a task as defined in this section. Therefore, multiparty physical access control may be achieved as specified in Section 5.1.2.1.

5.2.3 Identification and Authentication for Each Role

At all assurance levels other than Rudimentary, an individual shall identify and authenticate him or herself before being permitted to perform any actions set forth above for that role or identity.

5.2.4 Separation of Roles

Role separation, when required as set forth below, may be enforced either by the CA equipment, or procedurally, or both. Requirements for the separation of roles and limitations on use of procedural mechanisms to implement role separation for the TRCA and any subordinate CAs shall be as follows:

Table 5-1 Role Separation Rules

Assurance Level	Separation Rules
Rudimentary	No stipulation.
Basic	The CPS shall specifically designate individual CA personnel to the four roles defined in Section 5.2.1. In general, individuals may assume more than one role; however, no one individual shall assume both the Officer and Administrator roles. The DoT PKI CAs may enforce this procedurally. No individual shall have more than one identity.
Medium (all policies)	The CPS shall specifically designate individual CA personnel to the four roles defined in Section 5.2.1. Individuals may only assume one of the Officer, Administrator, and Auditor roles, but generally, any individual may assume the Operator role. The CA and RA software and hardware shall identify and authenticate its users and shall ensure that no user identity can assume both an Administrator and an Officer role, assume both the Administrator and Auditor roles, and/or assume both the Auditor and Officer roles. No individual shall have more than one identity.
High	The CPS shall specifically designate individual personnel to the four roles defined in Section 5.2.1. Individuals may assume only one of the Officer, Administrator, and Auditor roles. Generally, individuals designated as Officer or Administrator may also assume the Operator role. An auditor may not assume any other role. The CA and RA software and hardware shall identify and authenticate its users and shall enforce these roles. No individual shall have more than one identity.

Under no circumstances shall the incumbent of a CMA role perform its own external compliance auditor function. Only the CA Auditor may perform internal compliance auditor functions. The TRCA shall operate at the High Assurance level. The appropriate CPS designates the operating assurance level of individual subordinate CAs.

5.3 PERSONNEL CONTROLS

5.3.1 Background, Qualifications, Experience, & Security Clearance Requirements

The DoT PKI OA shall identify at least one individual or group responsible and accountable for the operation of each CA in the TCA. For the TRCA, these are the DoT PMO and the PKI OA.

Selection for any CMA or other DoT PKI trusted role is on the basis of loyalty, trustworthiness, and integrity. Trusted persons may be Department of the Treasury direct-hire personnel or contractors, but only U.S. citizens may fill trusted roles.

Only employees of the PKI Program Team shall fill DoT PKI CA trusted roles, unless specifically appointed by the PKI OA to satisfy operational requirements. Personnel appointed to the CA trusted roles shall meet the following requirements:

- Be employees of the Department of the Treasury, GS-5 (equivalent) or above, or equivalent contractor/vendor position of responsibility
- Have not been previously relieved of CMA related duties for reasons of negligence or non-performance of duties
- Have not been denied a security clearance, or had a security clearance revoked
- Have not been convicted of a felony offense
- Be appointed in writing by the DoT PKI OA
- PKI Program Team personnel acting in trusted roles for the Treasury Root and subordinate CAs appointed by the PKI OA, shall hold TOP SECRET security clearances.

5.3.2 Background Check Procedures

PKI Program Team and other designated personnel acting in RA trusted roles shall undergo, at a minimum, background check procedures necessary to be cleared for the TOP SECRET level. Information obtained from such checks, performed solely to determine the suitability of a person to fill a PKI role, are not releasable except as required in Section 9.4.

DoT PKI CA personnel shall pass, at a minimum, a background investigation covering the following areas:

- Employment
- Education
- Place of residence
- Law Enforcement

- References

The period of investigation must cover at least the last five years for each area, excepting the residence check, which must cover at least the last three years. Regardless of the date of award, the investigation shall verify the highest educational degree obtained.

A competent adjudication authority shall perform adjudication of the background investigation.

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of the DoT PKI CAs shall receive comprehensive training in all operational duties they will perform, including disaster recovery and business continuity procedures.

The PKI Program Team must ensure appropriate training for all personnel involved in CMA operations. Training will address the following topics:

- Operation of the CMA software and hardware
- CA operational and security procedures and mechanisms
- Stipulations of this policy and local guidance
- All PKI software versions in use
- All PKI duties personnel shall perform
- Disaster recovery and business continuity procedures

The specific training required will depend on the equipment used and the personnel selected. The PKI Program Team shall establish a training plan for a CMA installation. The PKI Program Team shall maintain documentation identifying all personnel who received training and the level of training completed. Where individuals demonstrated competence in lieu of training, the PKI Program Team shall maintain supporting documentation. CMA Training is the responsibility of the PKI Program Team, under the DoT PKI PMO.

5.3.4 Retraining Frequency & Requirements

Individuals responsible for PKI trusted roles shall be aware of changes in the DoT PKI CA operation. Any significant change to CMA operations shall have a training (awareness) plan, and the PKI Program Team shall document execution of such plans. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment. The PKI Program Team shall maintain documentation identifying all personnel who received training and the level of training completed.

5.3.5 Job Rotation Frequency & Sequence

This policy makes no stipulation regarding frequency or sequence of job rotation. Local policies that do impose such requirements shall provide for continuity and integrity of the PKI service.

5.3.6 Sanctions for Unauthorized Actions

A CMA shall report suspected security violations or compromises to the appropriate Security organization and the DoT PKI PMO so that the proper authorities may take appropriate administrative and/or disciplinary actions against personnel who violate applicable policy.

The DoT PKI OA shall take appropriate actions where personnel have performed actions involving the DoT PKI CAs or repositories not authorized in this CP, the appropriate CA CPS, or other procedures published by the DoT PKI PMO.

5.3.7 Independent Contractor Requirements

Contractor personnel employed to operate any part of the DoT PKI CAs or perform functions pertaining to the Department's PKI infrastructure shall be subject to the same criteria as a U.S. Government employee. Contractor personnel filling trusted roles shall be cleared to the TOP SECRET level. PKI subcontractors who provide services to the Department of the Treasury shall establish procedures to ensure that they perform in accordance with this policy.

5.3.8 Documentation Supplied To Personnel

Personnel filling trusted roles shall receive documentation sufficient to define duties and procedures for each role. This documentation includes, but is not limited to this CP; relevant portions of the applicable CPS, Contingency Plan, and KRPS; any relevant statutes, policies, and/or contracts; and any relevant programmatic documentation (e.g., CONOPS, Implementation Plan). Documentation may also include any handbooks, guidelines, or instructional manuals that have been or may be developed to ensure that personnel filling trusted roles are adequately trained.

5.4 AUDIT LOGGING PROCEDURES

DoT PKI CAs shall generate audit log files for all events relating to the security of the CAs. Where possible, the CAs shall automatically collect security audit log data. Where this is not possible, the CMA shall use a logbook, paper form, or other physical mechanism. The CMA shall retain and make available during compliance audits all security audit logs, both electronic and non-electronic. The CMA shall maintain the security audit logs for each auditable event defined in this section in accordance with retention period for archive, Section 5.5.2.

5.4.1 Types of Events Recorded

A message from any source received by the TCA requesting an action related to the operational state of a Treasury operated CA is an auditable event. The message must include message date and time, source, destination and contents. All security auditing capabilities of the CMA operating systems and applications required to meet this CP shall be enabled. As a result, most of the events identified in the table shall be automatically recorded. At a minimum, each audit record shall include the following (recorded either automatically or manually for each auditable event):

- The type of event

- The date and time the event occurred
- A success or failure indicator when executing the applicable TCA's signing process.
- A success or failure indicator when performing certificate revocation.
- Identity of the entity and/or operator (TCA personnel) that caused the event.

The table below lists detailed audit requirements according to the level of assurance. At a minimum, the CMA shall record (automatically or manually as appropriate) the events identified in the table for High Assurance.

Table 5-2 Auditable Event Requirements

Auditable Events (Logged either electronically or manually)	Rudimentary	Basic	Medium	High	PMA Auditor/or Script Required
SECURITY AUDIT					
Any changes to the Audit parameters, e.g., audit frequency, type of event audited		X	X	X	
Any attempt to delete or modify the Audit logs		X	X	X	
Obtaining a third-party time-stamp		X	X	X	
IDENTIFICATION AND AUTHENTICATION					
Successful and unsuccessful attempts to assume a role		X	X	X	
The value of maximum authentication attempts is changed		X	X	X	
Maximum authentication attempts unsuccessful authentication attempts occur during user login		X	X	X	
An Administrator unlocks an account that has been locked as a result of unsuccessful		X	X	X	

Table 5-2 Auditable Event Requirements					
Auditable Events (Logged either electronically or manually)	Rudimentary	Basic	Medium	High	PMA Auditor/or Script Required
authentication attempts					
An Administrator changes the type of authenticator, e.g., from password to biometrics		X	X	X	
LOCAL DATA ENTRY					
All security-relevant data that is entered in the system		X	X	X	X[2]
REMOTE DATA ENTRY					
All security-relevant messages that are received by the system		X	X	X	
DATA EXPORT AND OUTPUT					
All successful and unsuccessful requests for confidential and security-relevant information		X	X	X	
KEY GENERATION					
Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	X	X	X	X	X[1]
PRIVATE KEY LOAD AND STORAGE					
The loading of Component private keys	X	X	X	X	X[1]
All access to certificate subject private keys retained by the CA, RA, or LRA for key recovery purposes	X	X	X	X	
TRUSTED PUBLIC KEY					

Table 5-2 Auditable Event Requirements					
Auditable Events (Logged either electronically or manually)	Rudimentary	Basic	Medium	High	PMA Auditor/or Script Required
ENTRY, DELETION AND STORAGE					
All changes to the trusted public keys, including additions and deletions	X	X	X	X	
SECRET KEY STORAGE					
The manual entry of secret keys used for authentication			X	X	
PRIVATE AND SECRET KEY EXPORT					
The export of private and secret keys (keys used for a single session or message are excluded)	X	X	X	X	X[1]
CERTIFICATE REGISTRATION					
All certificate requests and handling	X	X	X	X	X[1]
CERTIFICATE REVOCATION					
All certificate revocation requests and handling		X	X	X	X[1]
CERTIFICATE STATUS CHANGE APPROVAL					
The approval or rejection of a certificate status change request		*X*	*X*	*X*	
CA, RA or LRA CONFIGURATION					
Any security-relevant changes to		X	X	X	X[1]

Table 5-2 Auditable Event Requirements					
Auditable Events (Logged either electronically or manually)	Rudimentary	Basic	Medium	High	PMA Auditor/or Script Required
the configuration of the CA or the RA					
ACCOUNT ADMINISTRATION					
Roles and users are added or deleted	X	X	X	X	
The access control privileges of a user account or a role are modified	X	X	X	X	
CERTIFICATE PROFILE MANAGEMENT					
All changes to the certificate profile	X	X	X	X	X[2]
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT					
All changes to the certificate revocation list profile		X	X	X	X[2]
MISCELLANEOUS					
Installation of the Operating System		X	X	X	X[1]
Installation of CA,, RA, or LRA Application		X	X	X	X[1]
Installing hardware cryptographic modules			X	X	X[1]
Removing hardware cryptographic modules			X	X	X[2]
Destruction of cryptographic		X	X	X	X[1]

Table 5-2 Auditable Event Requirements					
Auditable Events (Logged either electronically or manually)	Rudimentary	Basic	Medium	High	PMA Auditor/or Script Required
modules					
System Startup		X	X	X	
Logon Attempts on CA, RA, or LRA Applications		X	X	X	
Receipt of Hardware / Software			X	X	
Attempts to set passwords		X	X	X	
Attempts to modify passwords		X	X	X	
Backing up CA, RA. or LRA internal database		X	X	X	
Restoring* CA, RA, LRA internal database (*Auditor present with scripts for COOP Drills and Designated CA Disaster Recovery Events only. Auditor not required for high availability or normal switch over of services between facilities)		X	X	X	X[1]
File manipulation (e.g., creation, renaming, moving)			X	X	
Posting of any material to a repository			X	X	
Access to CA, RA, or LRA internal database			X	X	
All certificate compromise notification requests		X	X	X	
Loading tokens with certificates			X	X	X[1]
Shipment of Tokens			X	X	
Zeroize tokens		X	X	X	X[1]

Table 5-2 Auditable Event Requirements					
Auditable Events (Logged either electronically or manually)	Rudimentary	Basic	Medium	High	PMA Auditor/or Script Required
Rekey of the CA	X	X	X	X	X[1]
Configuration changes to the CA server, RA, or LRA involving:					
Hardware		X	X	X	X[1]
Software		X	X	X	X[1]
Operating System		X	X	X	X[2]
Patches		X	X	X	X[2]
Security Profiles			X	X	X[2]
PHYSICAL ACCESS / SITE SECURITY					
Personnel Access to room housing CA			X	X	
Access to the CA server			X	X	
Known or suspected violations of physical security		X	X	X	
ANOMALIES					
Software Error conditions		X	X	X	
Software check integrity failures		X	X	X	
Receipt of improper messages			X	X	
Misrouted messages			X	X	
Network attacks (suspected or confirmed)		X	X	X	
Equipment failure	X	X	X	X	

Table 5-2 Auditable Event Requirements					
Auditable Events (Logged either electronically or manually)	Rudimentary	Basic	Medium	High	PMA Auditor/or Script Required
Electrical power outages			X	X	
Uninterruptible Power Supply (UPS) failure			X	X	
Obvious and significant network service or access failures			X	X	
Violations of Certificate Policy	X	X	X	X	
Violations of Certification Practice Statement	X	X	X	X	
Resetting Operating System clock		X	X	X	

[1] Represents scripted events that are only related to certification authorities. Therefore, the PMA/Internal Auditor is required to be present during these activities. These events are considered significant architectural CA or are designated as controlled events within the TCA. Similar events related to Subscribers, RAs, LRAs, or TAs activities do not require the PMA/Internal Auditor to be present. However, the logging of all other identified auditable events in the table above will still be enforced either by electronic or manual processes as per policy.

[2] These events required configuration management and changes should be controlled through approved configuration change requests (CCRs). These scripts or CCRs will ensure that proper procedures are followed and to provide clear documentation of the changes made to the operational environment. These events are considered administrative in nature and therefore do not require the PMA/Internal Auditor to be present.

5.4.2 Frequency of Processing Log

Audit logs shall be retrieved and reviewed, by the Treasury PMA/Internal Auditor, in accordance with the table below and an audit alarm report shall be created by the PMA or Internal Auditor and submitted to the PMO for resolution. The Treasury PMO shall explain all significant events contained in the audit alarm report in an audit log summary. Such reviews involve verifying that the log has not been tampered with, and then inspecting a statistical set of all log entries, with a more thorough investigation of any alerts or irregularities contained within the logs. Actions taken because of these reviews shall be documented and reported to the PMA and any other appropriate authorities and entities in the same manner as outlined in Sections 8.5. The CMA

shall implement procedures to transfer the security audit data to secure storage before overwriting or overflow of automated security audit log files.

Table 5-3 Audit Log Review Schedule

Assurance Level	Audit Log Review Schedule
Rudimentary	Only required for cause
Basic	Only required for cause or as mandated by DoT security policy
Medium	At least once every two months (≤ 60 days) Statistically significant set of security audit data generated by the CA since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity. This amount will be described in the CPS.
High	At least once every month (≤ 30 days) Statistically significant set of security audit data generated by the CA since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity. This amount will be described in the CPS.

5.4.3 Retention Period for Audit Logs

For Medium, Medium Hardware, and High Assurance CAs, the CMA shall retain audit logs on-site until reviewed, as well as retaining such logs in the manner described in Section 5.5. The CMA-equipment shall retain the security audit information it generates for at least two months, as outlined in Section 5.4.4, 5.4.5 and 5.4.6, until moved to an appropriate archive facility.

An entity other than the CMA (i.e., officials different from the individuals who, in combination, command the CA signature key) shall delete the security audit data from the CMA-equipment. The CPS shall identify the archival entity. The CMA shall retain security audit data as archive records in accordance with Section 5.5.

5.4.4 Protection of Audit Logs

The security audit data shall not be open for reading or modification by any human, or by any automated process other than those that perform security audit processing. CMA must implement CA system configuration and procedures together to ensure that:

- Only personnel assigned to trusted roles have read access to the logs
- Only authorized people may modify, delete, or archive audit logs
- Audit logs are not modified

The entity performing security audit data archive need not have "Modify" access, but procedures must be implemented to protect archived data from deletion or destruction before the end of the security audit data retention period. The archival entity shall move security audit data to a safe, secure storage location separate from the CMA-equipment.

5.4.5 Audit Log Backup Procedures

The CMA shall backup audit logs and audit summaries at least monthly, and shall send a copy of the audit log off-site. The CMA shall protect the security audit data backup in accordance with the requirements of Section 5.4.4. CA Administrators/Security Officers/Operators shall both store and archive audit trail backup files in accordance with the PKI Backup and Restoration Procedures using the Department's standard backup utility.

5.4.6 Audit Collection System (internal vs. external)

The security audit process shall run independently, and the CMA shall not control it in any way. DoT PKI CAs shall invoke security audit processes (automated and manual) at system or application startup, and cease only at system or application shutdown. In the event that the automated security audit system fails, the CMA shall cease all operations, except for revocation processing, until it can restore the security audit capability. Under these circumstances, the CMA shall employ mechanisms to preclude unauthorized CMA functions. The CPS shall describe these mechanisms.

5.4.7 Notification to Event-Causing Subject

This CP imposes no requirement to notify an individual, organization, device, or application that caused an auditable event. This policy neither requires nor prohibits real-time alerts.

5.4.8 Vulnerability Assessments

The CMA, system administrator, and other operating personnel shall routinely assess whether the CA system or its components have been attacked, breached, or for attempts to violate the integrity of the certificate management system, including the equipment, physical location, and personnel.

The security auditor shall review security audit data for events such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses. Security auditors shall check for continuity of the security audit data.

5.5 RECORDS ARCHIVE

5.5.1 Types of Events Archived

CMA archive records[14] shall collect and maintain enough detail to establish the proper operation of the DoT PKI CAs, or the validity of any certificate (including revoked and/or expired) issued by the CA. At a minimum, the CMA shall archive following data, as well as all documentation required by compliance auditors:

Table 5-4 Data Archival Requirements

Data To Be Archived	Rudimentary	Basic	Medium (all policies)	High
CA accreditation (if applicable)	X	X	X	X
Certificate Policy and Certification Practice Statement	X	X	X	X
Any contractual agreements (as appropriate) to which the CMA is bound, and other agreements concerning operations of the CA	X	X	X	X
System and equipment configuration	X	X	X	X
Modifications and updates to system, configuration, documentation (e.g., CPS), and contractual agreements	X	X	X	X
Certificate requests	X	X	X	X
Revocation requests		X	X	X
Subscriber Identity Authentication data as per Section 3.2.3, and Subscriber agreements		X	X	X
Documentation of receipt and acceptance of certificates		X	X	X
Documentation of receipt of tokens		X	X	X
All certificates issued or published	X	X	X	X

[14] The term "archive" is not to be confused with a routine backup. The archive addressed in this section is a long-term, permanent storage of data that is critical as a historical record. See the terms "archive" and "backup" in this document's Glossary.

Table 5-4 Data Archival Requirements

Data To Be Archived	Rudimentary	Basic	Medium (all policies)	High
Record of CA Re-key and/or notification of cross certified CA Re-key in accordance with applicable MOAs	X	X	X	X
All CRLs issued and/or published		X	X	X
All Audit Logs, and security audit data and reports	X	X	X	X
Other data or applications to verify archive contents		X	X	X
All CA operations communications and documentation to the PMA, PKI PA, other CMAs, and compliance auditors		X	X	X

5.5.2 Retention Period for Archive

The minimum retention periods for archive data are identified below. Executive branch agencies must follow either the General Records Schedule established by the National Archives and Records Administration or an agency specific schedule as applicable. All other entities shall comply with their respective records retention policy in accordance with whatever law applies to that entity.

Table 5-5 Minimum Archive Retention Periods

Assurance Level	Retention Period
Rudimentary	7 Years 6 Months
Basic	7 Years 6 Months
Medium (all policies)	10 Years 6 months
High	20 Years 6 Months

5.5.3 Protection of Archive

Unauthorized users may not write to, modify, or delete the archive, but the CMA may move archived records to another medium as authorized by the PKI PMA. The CMA shall maintain a list of people authorized to modify or delete the archive from the system. Neither the CMA nor the archive site shall release the contents of the archive except: (1) in accordance with Department policy; or, (2) as required by law (See Sections 9.3 and 9.4). The CMA may release records of individual transactions upon request of any Subscribers involved in the transaction (i.e., originator or recipient), or their legally recognized agents.

Archive media shall be stored in a separate, safe, secure storage facility, not collocated with the DoT PKI CAs. Before archiving, the CMA shall label archive records with the distinguished name, the date, and the classification of the information. The DoT Data Archive Policy and Procedure shall contain procedures detailing how to create, package, and send archive information. Only authorized users may access the archive. The CMA will coordinate with Department Records Management Officials to ensure the scheduling and disposition approval by the NARA of all PKI archived records.

If the original media cannot retain the data for the required period, the PKI OA shall define a mechanism to transfer the archived data to new media periodically. The DoT PKI CAs shall provide archived data and the applications necessary to read the PKI archives to NARA or a Department of the Treasury approved archival facility for retention for at least the applicable retention period outlined above. DoT CAs shall also maintain collateral PKI data records, which are those records documenting the operation of the PKI but not directly related to the system used to generate keys, certificates, and so forth in a similar manner.

Alternatively, a DoT PKI CA may retain data using whatever procedures NARA has approved for that category of documents. The DoT CMAs shall also maintain applications required to process the archive data for a period determined by the PKI PMA.

Prior to the end of the archive retention period, the PKI OA shall provide archived data and the applications necessary to read the archives to a Department of the Treasury approved archival facility, which shall retain the applications necessary to read this archived data.

5.5.4 Archive Backup Procedures

The DoT Data Archive Policy and Procedure shall describe archive records back up, and archive backup management procedures.

5.5.5 Requirements for Time-Stamping of Records

DoT PKI CA archive records shall be automatically time-stamped as they are created. The CMA is responsible for assuring that time stamps are consistent with an authoritative time standard. The CPS shall describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

5.5.6 Archive Collection System (internal or external)

The DoT PKI CA systems, or the CMA staff, may collect archive data in any expedient manner, provide the collection process does not modify or delete the archive records and protects the data as outlined in Section 5.5.3.

5.5.7 Procedures to Obtain & Verify Archive Information

The DoT Data Archive Policy and Procedure shall describe procedures detailing how to create, verify, package, transmit, and store archive information.

The CMA shall not release the contents of the archive except as determined by the PMA or as required by law. The CMA or archive site may release records of individual transactions upon request of any Subscribers involved in the transaction, or their legally recognized agents.

5.6 KEY CHANGEOVER

CMAs must not issue Subscriber certificates that extend beyond the expiration dates of their own certificates and public keys. Each DoT PKI CA certificate validity period must extend one user certificate validity period past the last use of the CA private key. To minimize the risk to the PKI through compromise of an authority's key, the private signing key will change more frequently, and from that time on, certificate signing will use only the new key for certificate signing purposes. The older, but still valid, certificate will be available to verify old signatures until all of the user certificates signed under it have also expired. If the old private key signed CRLs that contain certificates also signed with that key, then the CMA must retain and protect the old key.

When a CA updates its private signature key and thus generates a new public key, the CA shall notify all CAs, RAs, and subscribers that rely on the CA's certificate that it has been changed. For the TRCA, key changeover procedures will establish key rollover certificates where the new private key signs a certificate containing the old public key, and the old private key signs a certificate containing the new public key.

The maximum validity period of the TRCA signature certificate is 35 years and the maximum lifetime of the associated private key is 15 years. The following table provides the maximum validity periods of CA signing keys and corresponding certificates:

Table 5-6 Maximum Validity Periods

Assurance Level	CA Signing Key/Certificate Validity Period (All values are in years)
Rudimentary	5/10

Table 5-6 Maximum Validity Periods

Assurance Level	CA Signing Key/Certificate Validity Period (All values are in years)
Basic	5/10
Medium (all policies)	3/8
High	3/8

RA key lifetimes are as described for Subscribers. If a CA certificate and key lifetime are shorter than a Subscriber's certificate and key lifetime, then the Subscriber certificate and key lifetime shall be no longer than that of the CA. DoT CAs may still use signature keys that have expired for the purposes of certificate signature for signing CRLs until the last Subscriber certificate signed using that key has expired.

5.7 COMPROMISE & DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

The DoT PMA shall notify the members of the Federal PKI Policy Authority, cross certified Entity CAs, and all subordinate CAs, if any, of the following cases occur:

- Suspected or detected compromise of TRCA systems;
- Physical or electronic attempts to penetrate TRCA systems;
- Denial of service attacks on TRCA components;
- Any incident preventing a TRCA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL.

This will allow other entities to protect their interests as Relying Parties.

The PKI Program Team shall reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the TRCA CPS.

Subordinate CAs shall notify the PKI PMO and all other subordinate CAs shall provide similar notice. Entity CAs, cross certified to a TRCA, shall provide notice to the DoT PKI PMO as required by the applicable MOA.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

When computing resources, software, and/or data are corrupted, the affected TRCA and subordinate CAs shall respond as follows:

- Before returning to operation, the CMA shall ensure that system integrity has been restored; and shall notify the PKI PMO and DoT PMA
- If the CA signature keys are not destroyed, CA operation shall be reestablished, giving priority to the ability to generate certificate status information within the CRL issuance schedule specified in Section 4.9.7.
- If the CA signature keys are destroyed, CA operation shall be reestablished as quickly as possible, giving priority to the generation of a new CA key pair.

5.7.3 Entity (CA) Procedures

In case of a CA key compromise or loss (such that compromise is possible even though uncertain) involving the TRCA:

- The DoT PMA shall immediately notify the FPKIPA and all of its member entities so that those entities may issue CRLs revoking any cross certificates issued to the TRCA
- The TRCA CMA must remove the trusted self-signed certificate from each Relying Party application, and shall distribute a new one via secure out-of-band mechanisms. The TRCA will describe its approach to reacting to a TRCA key compromise in its CPS.
- The PKI Program Team may generate a new TRCA key pair in accordance with procedures set forth in the TRCA CPS if so determined by the PMA
- The PKI Program Team may also issue new TRCA certificates to the FBCA and all cross certified Entities in accordance with the TRCA CPS. If the CA distributes its key in a trusted certificate, the CMA shall distribute the new trusted certificate as specified in Section 6.1.4.

In case of a CA key compromise or loss involving a subordinate CA:

- The TRCA shall revoke that CA's certificate, and publish the revocation information immediately in the most expedient manner
- The TRCA shall re-establish the subordinate CA installation as outlined herein
- The FPKIPA and all of its member entities shall be notified
- If re-establishment is directed, the CMA shall generate a new CA key pair in accordance with procedures set forth in the appropriate CPS
- Upon re-establishment, the CMA shall issue new CA certificates to Entities also in accordance with the affected CA CPS

The PKI OA shall also investigate and report to the DoT PMA what caused the compromise or loss, and what measures have been taken to preclude recurrence.

5.7.4 Business Continuity Capabilities after a Disaster

The PKI OA shall maintain a Disaster Recovery Plan and shall operate a warm backup site, whose purpose is to ensure continuity of operations in the event of failure of the primary site.

DoT PKI CA operations shall be designed to restore full service within six hours of primary system failure. DoT shall deploy the PKI CA directory system to provide 24 hour, 365 day per year availability. The PKI PMO shall implement features to provide high levels of directory reliability within the scope of its control.

In the case of a disaster damaging or rendering all CA equipment inoperative, the PKI Program Team shall re-establish affected CA operations as quickly as possible, giving priority to the ability to revoke certificates, regardless of type or user. For the TRCA, this will require secure out-of-band distribution of the new certificate as well as issuance of new cross certificates, subordinate CA certificates, and Subscriber certificates.

The PMA shall, at the earliest feasible time, securely advise the FPKIPA and all of its member entities in the event of a disaster where the TRCA installations are physically damaged and all copies of the TRCA' signature keys are destroyed. Relying Parties may decide of their own volition whether to continue to use certificates signed with the destroyed private key pending reestablishment of TRCA operation with new certificates.

In the case of a disaster causing physical damage to a subordinate CA installation and resulting in destruction of all copies of the CA signature key, the subordinate CA shall request revocation of its certificates. The PKI Program Team will then completely rebuild the CA installation by reestablishing the CA equipment, generating new private and public keys, be re-certified, and re-issue all cross certificates. Finally, all Subscriber certificates will be re-issued. Relying parties may make a judgment to continue to use certificates signed with the destroyed private key in order to meet urgent operational requirements. In any event, the PMA shall securely notify all appropriate authorities (e.g., the FPKIPA, FBCA, cross certified CAs, etc.) of the situation at the earliest feasible time in accordance with applicable MOAs and any other contractual agreements.

If a CA's signature keys are compromised, lost, or destroyed—such that compromise is possible even though uncertain—the PKI OA shall cause an investigation to be conducted and report to the PMA concerning the cause of the compromise or loss and what measures have been taken to prevent recurrence. The PMA, in turn, will notify the appropriate authorities in accordance with applicable MOAs and any other contractual agreements.

5.8 CA & RA TERMINATION

DoT PKI CA termination will precede in accordance with Section 9.10. In the event of termination of the TRCA operation, certificates signed by the TRCA shall be revoked and the DoT PMA shall advise entities that have entered into MOAs with the Department's PKI that the TRCA operation has terminated so they may revoke certificates they have issued to the TRCA. Prior to TRCA termination, the PKI OA shall provide all archived data to an archival facility. CMAs shall give cross certified entities as much advance notice as circumstances permit, and attempt to provide alternative sources of interoperation in the event the supporting TRCA is terminated.

In the case of subordinate CAs, if the termination is for convenience, contract expiration, re-organization, or other non-security related reason, and provisions have been made to continue compromise recovery, compliance and security audit, archive, and data recovery services, then

neither the terminated CA's certificate, nor certificates signed by that CA, need to be revoked. If provisions for maintaining these services cannot be made, then the CA termination will be handled as a CA compromise in accordance with Section 4.9. Before termination, the PMA shall securely notify all appropriate authorities (e.g., the FBCA, cross certified CAs, etc.) of the situation at the earliest feasible time in accordance with applicable MOAs and any other contractual agreements.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION & INSTALLATION

6.1.1 Key Pair Generation

This policy does not preclude any source of key generated in accordance with the stipulations of this policy and local security requirements. A private key must not appear outside of the module in which generated unless encrypted for local transmission or for processing or storage by a key recovery mechanism. Section 6.1.1.1 defines requirements for cryptographic modules used for key generation and storage.

6.1.1.1 CA Key Pair Generation

The Treasury TRCA, subordinate CAs, and OCSPs shall generate cryptographic keying material used to sign certificates, CRLs or status information in FIPS 140 validated cryptographic modules. CA cryptographic modules shall meet or exceed FIPS 140 Security Level 3. Multiparty control is required for CA key pair generation, as specified in Section 5.2.2.

The Treasury Root and subordinate CAs must document their key generation procedure in their respective CPSs, and generate auditable evidence that they followed the documented procedures. For all levels of assurance, the documentation of the procedure must provide enough detail to show the use of appropriate role separation. For High, Medium Hardware, and Medium assurance, an independent third party shall validate the process either by witnessing or by examining the signed and documented procedures.

6.1.1.2 Subscriber Key Pair Generation

The Subscriber, RA, or CA may perform Subscriber key pair generation. If the CA or RA generates Subscriber key pairs, the procedure must meet the requirements for key pair delivery specified in Section 6.1.2. All key generation shall be performed using a FIPS approved method.

At the High and Medium Hardware assurance levels, the Subscriber, RA, or CA shall generate the Subscriber key pairs in hardware cryptographic modules validated to FIPS 140 Level 2 or above. For all other assurance levels, the Subscriber, RA, or CA may use either validated software or hardware cryptographic modules for key generation.

6.1.2 Private Key Delivery to Subscriber

If Subscribers generate their own key pairs, then there is no need to deliver private keys, and this section does not apply. If an Entity other than the Subscriber generates a private key, the CMA shall deliver the key to the Subscriber electronically or in a hardware token from which the private key cannot be extracted in unencrypted form. Any transmission of a private key over a network must use be encrypted.

In those cases where a DoT PKI CA generates public/private key pairs on behalf of the Subscriber, the CA shall implement mechanisms to ensure that the public/private key pair is securely delivered to the proper Subscriber. The appropriate CPS describes this method.

For High and Medium Hardware assurance, a private key will be generated and must remain within the cryptographic boundary of the cryptographic module. If the CMA generates the key, then the CMA must also deliver the key module to the Subscriber. The Subscriber shall formally acknowledge receipt of the module. The CMA must maintain a record of the Subscriber acknowledgement of receipt of the token.

Under no circumstances shall any entity other than the Subscriber have knowledge of private signing keys. In the case of tokens (e.g., smart cards) the CA shall also implement procedures to ensure that the token is not activated by an unauthorized Entity. The CMA must send any key management private keys that are to be delivered over a network, encrypted and directly to the Subscriber's cryptographic module.

In all cases, the following requirements must be met:

- No one who generates a private signing key for a Subscriber shall retain any copy of the key after delivery of the private key to the Subscriber.
- The private key must be protected from activation, compromise, or modification during the delivery process.
- The Subscriber shall acknowledge receipt of the private key(s), regardless of the delivery means.
- Delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers.
  - For hardware modules, accountability for the location and state of the module must be maintained until the Subscriber accepts possession of it.
  - For electronic delivery of private keys, the key material shall be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data shall be delivered using a separate secure means.
  - For shared key applications, organizational identities, and network devices, see also Sections 3.2 and 3.3.

6.1.3 Public Key Delivery to Certificate Issuer

For DoT PKI CAs operating at the Basic, Medium, Medium Hardware, or High level of assurance, the following requirements apply:

- Where key pairs are generated by the Subscriber or RA, the public key and the Subscriber's identity must be delivered securely to the CA for certificate issuance.
- The delivery mechanism shall bind the Subscriber's verified identity to the public key. If cryptography is used to achieve this binding, it must be at least as strong as the CA keys used to sign the certificate. Alternatively, this binding may be accomplished through in-person appearance before the RA, LRA, or trusted agent.

For Rudimentary Assurance, this CP makes no stipulation.

The CMA shall deliver public keys to the certificate issuer in an authenticated manner set forth in the CPS.

6.1.4 CA Public Key Delivery to Relying Parties

When a CA updates its signature key pair, the CA shall distribute the new public key in a secure fashion. The CA may distribute the new public key in a self-signed certificate, in a key rollover certificate, or in a new CA (e.g., cross) certificate obtained from the issuer(s) of the current CA certificate(s).

TRCA shall make their public keys available for creation and verification of certification trust paths, in the form of a self-signed public-key certificate. The CA shall deliver this self-signed certificate to Subscribers in a manner commensurate with the security offered by the public key in the certificate. CAs shall convey self-signed certificates to relying parties in a secure fashion to preclude substitution attacks. Such methods include, but are not limited to the following:

- Loading a self-signed certificate onto tokens delivered to Relying Parties via secure mechanisms
- Distribution of self-signed certificates through secure out-of-band mechanisms
- Comparison of certificate hashes against trusted certificate hashes made available via authenticated out-of-band sources (note that hashes posted in-band along with the certificate are not acceptable as an authentication mechanism)
- Downloading certificates from web sites secured with a currently valid certificate of equal or greater assurance level than the certificate downloaded

The CA shall sign the key rollover certificates with the CA's current private key, so secure distribution is not required.

6.1.5 Key Sizes

This CP requires the use of RSA PKCS#1, RSA-PSS, or ECDSA signatures; additional implementation restrictions on key sizes and hash algorithms are specified below. Certificates issued under this policy shall contain RSA or elliptic curve public keys. Future revisions of this CP may specify any FIPS-approved signature algorithms that are considered acceptable. If the Treasury PMO determines that the security of a particular algorithm may have been compromised, the TCA shall revoke all certificates signed by or asserting the compromised algorithm.

The key size requirements set forth in this section apply to both the CA signing key pair and the subscriber key pair. Treasury Subscriber certificates issued for assurance levels Rudimentary through Medium, and that expire on or before December 31, 2010 shall use at least 1024 bit RSA, DSA or Diffie Hellman (DH) and Secure Hash Algorithm version 1 (SHA-1 or better) in accordance with FIPS 186. Subscriber certificates issued under id-fpki-common-policy will comply with Federal PKI Common Policy Framework.

For CAs that distribute self-signed certificates to relying parties, the CA's subject public keys in such certificates shall be at least 2048 bits for RSA, or at least 224 bits for ECDSA.

CAs that generate certificates and CRLs under this policy shall use signature keys of at least 1024 bits for RSA or DSA, and at least 160 bits for ECDSA. Certificates that expire after 12/31/2010 shall be generated with at least 2048 bit RSA key, or at least 224 bits for ECDSA.

CAs that generate certificates and CRLs under this policy shall use SHA-1, SHA-224, SHA-256, SHA-384, or SHA-512 hash algorithm when generating digital signatures. CAs generating signatures on certificates and CRLs issued after 12/31/2010 shall use, at a minimum, SHA-256.

Where implemented, CSSs shall sign responses using the same signature algorithm, key size, and hash algorithm used by the CA to sign CRLs.

End-entity certificates shall contain public keys that are at least 1024 bits for RSA, DSA, or Diffie-Hellman, or 160 bits for elliptic curve algorithms.

- End-entity certificates that include a key usage extension asserting only the digital signature bit, and that expire on or after 12/31/2013 shall contain public keys that are at least 2048 bits for RSA or Diffie-Hellman, or 224 bits for elliptic curve algorithms.
- End-entity certificates that do not include a key usage extension or that include a key usage extension that asserts the *nonRepudiation, keyEncipherment, dataEncipherment,* or *keyAgreement* bit, and that expire on or after 12/31/2010 shall contain public keys that are at least 2048 bits for RSA or Diffie-Hellman, or 224 bits for elliptic curve algorithms.

Use of SSL/TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum AES (128 bits) or equivalent for the symmetric key, and at least 1024 bit RSA or 163 bit elliptic curve keys through 12/31/10 for asymmetric keys issued under assurance levels Rudimentary through MediumHardware and 2048 bit RSA or equivalent for the asymmetric keys issued under High assurance and on or after 12/31/2010 at least 2048 bit RSA or 224 bit elliptic curve keys will be utilized by the protocol for all assurance levels.

6.1.6 Public Key Parameters Generation and Quality Checking

DoT PKI CAs shall generate public key parameters for signature algorithms defined in the Digital Signature Standard (DSS) in accordance with FIPS 186. The CMA shall generate and test public key parameters in accordance with the standard that defines the cryptographic algorithm in which the parameters are used.

Using automated testing features within the cryptographic module or kernel, or the system, the CMA shall generate and test public key parameters for Digital Signature Algorithm (DSA) in accordance with the *Digital Signature Standard* FIPS-186. The CMA shall also test prime numbers for KEA and RSA for determination of whether they are prime using FIPS 186, or tests that are more stringent.

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

DoT CAs shall certify public keys bound into certificates for use in signing or encrypting, but not both, except as specified below. The key usage extension in the X.509 certificate determines the use of a specific key. With the exception of the self-signed TRCA certificate, all certificates must have a populated key usage extension as defined in the X.509 key usage extensions. The key usage extension in the X.509 certificate determines the use of a specific key. Subordinate CAs shall set at least two key usage bits: *cRLSign* and *keyCertSign*. Where the subject signs OCSP responses, the certificate may also set the *digitalSignature* and/or *nonRepudiation* bits.

Subscriber certificates shall assert key usages based on the intended application of the key pair. Subscriber certificates to be used for digital signatures (including authentication) shall set the *digitalSignature* and/or *nonRepudiation* bits. However, a public-key certificate with key usage set for *digitalSignature* and *keyEncipherment* shall not also set for *nonRepudiation*. Certificates issued only for Authentication shall only set the *digitalSignature* bit. Certificates to be used for key or data encryption shall set the *keyEncipherment* and/or *dataEncipherment* bits. Certificates used for key encryption shall set the *keyAgreement* bit if the algorithm is DH and shall set the *keyEncipherment* bit if the algorithm is RSA. This restriction does not prohibit use of protocols that provide authenticated connections using key management certificates. Certificates to be used for key agreement shall set the *keyAgreement* bit.

Rudimentary, Basic, and Medium Assurance Level certificates may include a single key for use with encryption and signature in support of legacy applications. DoT PKI CAs shall generate and manage such dual-use certificates in accordance with their respective signature certificate requirements, except where otherwise noted in this CP. Such dual-use certificates shall never assert the non-repudiation key usage bit, and shall not be used for authenticating data that will be verified on the basis of the dual-use certificate at a future time. DoT CAs shall issue Subscribers at all levels of assurance two key pairs; one for key management and one for digital signature, except where operationally necessary (e.g., VPN and web site/application access control). This restriction does not prohibit use of protocols that provide authenticated connections using key management certificates.

6.2 PRIVATE KEY PROTECTION & CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards & Controls

The relevant standard for cryptographic modules is FIPS 140, *Security Requirements for Cryptographic Modules*.

NIST shall validate cryptographic modules to the FIPS 140 level identified in this section. Additionally, the Department of the Treasury reserves the right to review technical documentation associated with any cryptographic modules under consideration for use by the DoT PKI CAs.

The following table specifies the minimum level of FIPS evaluation a cryptographic module must complete for use in the Department of the Treasury PKI:

Table 6-1 Minimum Level of FIPS Evaluation

Assurance Level	CA & CSS	Subscriber	RA
Rudimentary	Level 1 (Hardware or Software)	N/A	Level 1 (Hardware or Software)
Basic	Level 2 (Hardware or Software)	Level 1 (Hardware or Software)	Level 1 (Hardware or Software)
Medium	Level 2 (Hardware)	Level 1 (Hardware or Software)	Level 2 (Hardware)
Medium Hardware	Level 2 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)
High	Level 3 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)

The TRCA require Level 3 cryptographic modules as defined by FIPS 140. The TRCA may use a higher level if available or desired. Subordinate CAs shall sign certificates using a cryptographic module that meets Level 3 or higher. RAs shall use hardware cryptographic modules at Level 2 or higher. For Medium and High assurance levels, Subscribers shall use FIPS 140 Level 2 or higher validated hardware cryptographic modules (tokens).

All cryptographic modules shall operate such that the private asymmetric cryptographic keys never output in plain text. No private key shall appear unencrypted outside the CA equipment. No one shall have access to a private signing key but the subject of the corresponding certificate.

6.2.2 Private Key Multi-Person Control

Use of the TRCA private signing keys shall require action by multiple persons as set forth in Section 5.2.2 of this CP. Use of subordinate CAs private signing keys shall require action by multiple persons at Medium, Medium Hardware, and High Assurance as set forth in Section 5.2.2 of this CP.

Access to Medium, Medium Hardware, and High CA cryptographic modules shall be under two-person control. CMAs shall also back up key management and signature keys in multiple cryptographic modules under two-person control and ensure the security audit records the CMA backup actions. Only a CA may reproduce private keys in multiple cryptographic modules on behalf of Subscribers; neither RAs nor Subscribers shall duplicate private keys. The CMA may backup DoT CA signature keys only under two-person control. The CMA shall maintain a list of names of the parties used for two-person control.

6.2.3 Private Key Escrow

6.2.3.1 Escrow of TRCA and Subordinate CA private signature keys

Under no circumstances shall TRCA or subordinate CA signature keys used to sign certificates or CRLs be escrowed.

6.2.3.2 Escrow of CA Encryption Keys

TRCA shall not perform any encryption key recovery functions involving encryption keys issued to subordinate CAs. However, if encryption key pairs need to be issued by the TRCA covering repository system access or for other purposes, the DoT PMA shall publish applicable requirements for that purpose.

Subordinate CAs may escrow any encryption keys whose certificates do not contain the *digitalSignature* key usage bit for the purpose of data recovery. The applicable CA CPS shall describe this method.

6.2.3.3 Escrow of Subscriber private signature keys

Subscriber private signature keys shall not be escrowed.

6.2.3.4 Escrow of Subscriber private encryption and dual use keys

Subscriber private dual use keys shall not be escrowed. Subordinate CAs may escrow any encryption keys whose certificates do not also contain the *digitalSignature* key usage bit for the purpose of data recovery. Keys in escrow must be protected using cryptography validated to the same FIPS level as the CA. Recovery of keys in escrow must be protected using the same level of strength of technical controls present at the time of initial issuance, which are described in section 6.1.2.

6.2.4 Private Key Backup

6.2.4.1 Backup of TRCA and Subordinate CA Private Signature Keys

The TRCA shall back up private signature keys under multi-person control, as specified in Section 5.2.2. Backup of subordinate CA private signature keys is required to facilitate disaster recovery. Where required by Section 5.2.2, subordinate CAs shall back up private signature keys under multi-person control.

The CMA shall create backups of the TRCA and subordinate CA private signature keys on separate cryptographic modules. The CMA shall create these keys under the same multi-person control as the original signature key. Such backups shall create only a single copy of the TRCA and subordinate CA signature key at the primary CA location. The CA shall store at least one copy of each TRCA and each subordinate CA private signature key at the off-site backup location. The CMA shall account for and protect all copies of CA private signature keys in the same manner as the original.

All backup copies of CA private signature keys shall reside solely on cryptographic modules of equal strength and validation level as the primary. These levels are detailed in section 6.2.1

6.2.4.2 Backup of Subscriber private signature key

The backup, copying, or escrow of Subscriber private signature keys is prohibited.

6.2.4.3 Backup of Subscriber Key Management Private Keys

Subordinate CAs may backup Subscriber key management private keys.

Subordinate CAs must encrypt backed up Subscriber key management private keys using an algorithm of a strength consistent with the private key being stored; or stored in a cryptographic module validated at FIPS 140 Level 2.

6.2.4.4 Backup of CSS Private Key

DoT CMAs may backup CSS private keys. If backed up, the CMA shall account for and protect all copies in the same manner as the original.

6.2.5 Private Key Archival

DoT CAs shall not escrow or archive private signature keys as outlined in Section 6.2.3. Subordinate CAs may escrow or archive private encryption keys (key management or key transport) as outlined in Section 6.2.3.

6.2.6 Private Key Transfer into or from a Cryptographic Module

TRCA and subordinate CA private keys shall be generated by and remain within a cryptographic module. At no time shall the CA private key exist in plain text outside the cryptographic module. The CMA may backup CA private keys in accordance with Section 6.2.4.1.

Subscriber private keys must be generated by and remain within a cryptographic module. In the event that a CMA transports a private key from one cryptographic module to another, the private key must be encrypted during transport. Private keys must never exist in plain text form outside the cryptographic module boundary.

The system must protect private or symmetric keys used to encrypt other private keys for transport, from disclosure. The protection of these keys must be commensurate with that provided the data protected by the certificate associated with the private key.

6.2.7 Private Key Storage on Cryptographic Module

This CP makes no further stipulation beyond that specified in FIPS 140.

6.2.8 Method of Activating Private Keys

For the TRCA and subordinate CAs that operate at the Medium, Medium Hardware, or High level of assurance, CA signing key activation requires multiparty control as specified in Section 5.2.2.

Subscribers must use pass-phrases, PINS, biometric data, or other mechanisms of equivalent authentication robustness to authenticate to the cryptographic module before activating any private key in the cryptographic module for certificates at all levels of assurance[15]. Section 6.4.1 specifies activation data generation requirements. The CMA must distribute activation data in person, or by an accountable method to the Subscribers separately from the cryptographic modules that they activate. Subscribers must protect the entry of activation data from disclosure using protections described in section 6.4.2.

6.2.9 Methods of Deactivating Private Keys

The CMA shall remove TRCA and subordinate CA cryptographic modules and store them in a secure container when not in use, as specified in Section 5.1.2.

Subscribers shall not leave activated cryptographic modules unattended or otherwise open to unauthorized access. When not in active use, they must be deactivated, e.g. via a manual logout procedure, by removing the cryptographic module, or automatically after a period of inactivity as defined in the applicable CA CPS. Subscribers shall remove and secure (e.g., under their personal control or in an approved security container) cryptographic modules when not in use.

6.2.10 Method of Destroying Private Keys

Individuals in trusted roles shall destroy CA, RA, and status server (e.g., OCSP server) private signature keys when no longer needed. Subscriber private signature keys shall be destroyed when no longer needed, or when the certificates to which they correspond expire or are revoked. For software cryptographic modules, this can be overwriting the data using a DoT-approved utility and procedures. For hardware cryptographic modules, this will likely be executing a "zeroize" command. Private key destruction should not require physical destruction of hardware.

PKI Sponsors shall request the assistance of the LRA, RA, or CMA with the overwriting of software cryptographic modules used by hardware components and applications. Individual Subscribers shall take hardware tokens to the LRA, RA, or CMA for zeroizing to prevent accidental destruction of Access Control System or other resident data kept on the Smart ID Card/PIV Card.

6.2.11 Cryptographic Module Rating

See Section 6.2.1

[15] For certificates issued at the Card Authentication level of assurance, Subscriber authentication is not required to use the associated private key.

6.3 OTHER ASPECTS OF KEY MANAGEMENT

A single dual-use (digital signature and encryption) key pair is prohibited for Medium Hardware and High Assurance implementations, but may be issued on a case-by-case basis for Rudimentary, Basic, and Medium Assurance levels. Such dual-use key pairs shall be issued only in support of legacy applications as defined in Section 6.1.7. Human Subscribers shall typically have one key-pair for digital signature, and a separate key-pair for encryption. A Subscriber's digital signature key-pair shall never be escrowed, archived, or backed-up, to maintain technical non-repudiation of transactions. For business continuity reasons, the CA may escrow, archive, or back-up encryption key-pairs.

6.3.1 Public Key Archival

The public key is archived as part of the certificate archival.

6.3.2 Certificate Operational Periods/Key Usage Periods

DoT CAs that distribute their self-signed certificates for use as trust anchors shall limit the use of its private keys to a maximum of 20 years; the self-signed certificates shall have a lifetime not to exceed 37 years. For all other CAs, the CA shall limit the use of its private keys to a maximum of four years for Subscriber certificates and ten years for CRL signing and OCSP responder certificates. Code and content signers shall use their private keys for a maximum of three years; the lifetime of the associated public keys shall not exceed eight years. Subscriber signature private keys and certificates shall have a maximum lifetime of three years. Signatures generated with these keys may be validated after expiration of the certificate. Subscriber key management certificates shall have a maximum lifetime of 3 years; use of Subscriber key management private keys is unrestricted. All restrictions on private-key usage periods are enforced procedurally.

Subscriber public keys in certificates that assert the id-PIV-content-signing OID in the extended key usage extension have a maximum usage period of eight years. The private keys corresponding to the public keys in these certificates have a maximum usage period of three years.

The validity period of the Subscriber certificate must not exceed the routine re-key Identity Requirements as specified in Section 3.3.1. Section 5.6, as well as the CPS, describes the key usage periods for keying material.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation & Installation

The activation data used to unlock TRCA, subordinate CA or Subscriber private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data protected. If the activation data must be transmitted, it shall be via an appropriately protected channel, and separate in time and place from the associated cryptographic module. Where the TRCA or a subordinate CA uses passwords as activation data for the CA signing key, the CMA shall change the activation data upon CA re-key at a minimum.

The activation data used by Subscribers to unlock private keys shall have an appropriate level of strength for the keys or data protected. Subscribers shall use pass-phrases, PINS, biometric data, or other mechanisms of equivalent authentication robustness to protect access to use of a private key for certificates at all other levels of assurance[16].

6.4.2 Activation Data Protection

Subscribers shall protect data used to unlock private keys from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data shall be:

- Memorized
- Biometric in nature, or
- Recorded and secured at the level of assurance associated with the activation of the cryptographic module, and shall not be stored with the cryptographic module.

The protection mechanism shall include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as set forth in the respective CPS.

Subscribers must never share activation data for private keys associated with certificates asserting individual identities. PKI Sponsors shall restrict activation data for private keys associated with certificates asserting group, organizational, non-human component identities to those in the organization authorized to use the private keys.

If transmission of the activation data must occur, it shall be via a channel with appropriate protection, and distinct in time and place from the associated cryptographic module. As part of the delivery method, users will sign and return a delivery receipt. In addition, users will also receive (and acknowledge) a user advisory statement to help to understand responsibilities for use and control of the cryptographic module.

6.4.3 Other Aspects of Activation Data

When operating at a Medium Hardware or High assurance level, RAs shall change their cryptographic module activation data not less than once every six months.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

For all DoT PKI CAs, the computer security functions listed below are required. These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. CAs and ancillary parts shall include the following functionality:

- Require authenticated logins

[16] For certificates issued at the Card Authentication level of assurance, Subscriber authentication is not required to use the associated private key.

- Provide Discretionary Access Control
- Provide a security audit capability
- Restrict access control to DoT PKI CA services and PKI roles
- Enforce separation of duties for PKI roles
- Require identification and authentication of PKI roles and associated identities
- Prohibit object re-use or require separation for CA random access memory
- Require use of cryptography for session communication and database security
- Archive CA history and audit data
- Require self-test security related CA services
- Require a trusted path for identification of PKI roles and associated identities
- Require recovery mechanisms for keys and the CA system
- Enforce domain integrity boundaries for security critical processes and provide process isolation, operating system self-protection, and residual information protection

For subordinate CAs, the computer security functions listed below are also required. These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. Subordinate CAs and ancillary parts shall include the following functionality:

- Authenticate the identity of Subscribers before permitting access to the system or applications
- Manage privileges of Subscribers to limit Subscribers to their assigned roles
- Generate and archive audit records for all transactions (see Section 5.4)
- Enforce domain integrity boundaries for security critical processes
- Support recovery from key or system failure

For Certificate Status Servers (CSS) operating under this policy, the computer security functions listed below are required:

- Authenticate the identity of users before permitting access to the system or applications
- Manage privileges of users to limit users to their assigned roles
- Enforce domain integrity boundaries for security critical processes and provide process isolation, operating system self-protection, and residual information protection
- Support recovery from key or system failure

6.5.2 Computer Security Rating

When evaluated platforms host CA equipment in support of computer security assurance requirements, then the system (hardware, software, and operating system) shall operate only in an evaluated and certified configuration, per the Department of the Treasury Office of Cyber Security. At a minimum, such platforms shall use the same version of the computer operating system as received the evaluation rating.

6.6 LIFE-CYCLE SECURITY CONTROLS

6.6.1 System Development Controls

The System Development Controls for the TRCA and subordinate CAs at the Basic Assurance level and above are as follows:

- The CAs shall use software designed and developed under a formal, documented development methodology.
- The CA shall use hardware and software specifically developed in a controlled environment; and the CMA shall define and document the development process. This requirement does not apply to commercial off-the-shelf (COTS) hardware or software.
- Where developers use open source software, the developer/vendor shall demonstrate that security requirements were achieved through software verification & validation and structured development/life-cycle management.
- The PKI Program Team shall procure hardware and software to operate the CA in a fashion to reduce the likelihood of tampering with any particular component (e.g., by ensuring the random selection of material at time of purchase).
- The PKI Program Team shall dedicate CA hardware and software to performing one task: operation and management of the CA. There shall be no other applications, hardware devices, network connections, or component software installed that are not part of the CA operation.
- The PKI Program Team shall take proper care to prevent malicious software from being loaded onto the CA equipment. RA hardware and software shall be similarly limited and scanned for malicious code on first use and continuously thereafter.
- Hardware and software updates shall be purchased or developed in the same manner as original equipment, and shall be installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

The PKI Program Team shall document and control the configuration of all CA systems as well as any modifications and upgrades. There shall be a mechanism for detecting unauthorized modification to the CA software or configuration. The PKI Program Team shall use the Department's formal configuration management methodology, through the IT-CCB, for installation and ongoing maintenance of the DoT PKI CA systems. The PKI OA shall verify the

CA software, when first loaded, as that supplied from the vendor, with no modifications, and the version intended for use. The operator shall verify the integrity of CA software at least weekly.

6.6.3 Life Cycle Security Ratings

This CP makes no stipulation.

6.7 NETWORK SECURITY CONTROLS

The PKI CMAs shall employ network security controls to protect the TRCA, the TRCA certificate repositories, and Certificate Status Servers. The CMA shall assure that all CMA equipment is protected (e.g., network guard, firewall, and/or filtering router) against known network attacks. The DoT PKI CA system administrator shall turn off all unused network ports and services on the CAs, and ensure that similar measures are taken on all guards, routers, and firewalls. Any network software present on CMA equipment shall be necessary to the functioning of the CMA application.

Subordinate CAs, RAs, and supporting directories and certificate status servers shall employ the same network security controls required of the TRCA, appropriate to their configuration.

- The DoT Border Directory shall be connected to the Internet and provide continuous service (except, when necessary, for brief periods of maintenance or backup) as outlined in Section 2.2.1. Any boundary control devices used to protect the Border directory or any CA local area network shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network. All boundary control devices shall only have user accounts required to administer the boundary control protections. The TRCA CPS shall define the respective network protocols and mechanisms required for operation of the Border Directory.
- The TRCA is operated off-line; CRLs and ARLs are posted manually to the directories.

6.8 TIME STAMPING

Asserted times shall be accurate to within three minutes. The PKI Program Team may use electronic or manual procedures to maintain system time. Clock adjustments are auditable events, see Section 5.4.1.

7. CERTIFICATE, CARL/CRL, & OCSP PROFILES FORMAT

7.1 CERTIFICATE PROFILE

The FPKI PROF defines the Certificate Profile. The certificate profile that the Department will use conforms to the FPKI Certificate and CRL profiles as defined in the current *Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile* [FPKI-Prof].

7.1.1 Version Numbers

This policy uses X.509 Version 3 certificates exclusively.

The TRCA and subordinate CAs shall issue X.509 v3 certificates.

7.1.2 Certificate Extensions

For all CAs, use of standard certificate extensions shall comply with [RFC 3280]. Certificates issued by the TRCA shall comply with Federal Public Key Infrastructure X.509 Certificate and CRL Extensions Profile [FPKI-Prof]. Certificates issued by subordinate CAs operating at High, Medium Hardware, and/or Medium Assurance shall also comply with [FPKI-Prof]. PIV Authentication Certificates issued by a subordinate CA under this policy may conform to the X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program [CCP-PROF] instead.

Certificates issued by the TRCA shall not include critical private extensions. Subscriber certificates issued by subordinate CAs may include critical private extensions so long as interoperability within the community of use is not impaired. For PIV Auth certificates, the [CCP-Prof] defines the rules for the inclusion, assignment of value, and processing of extensions.

7.1.3 Algorithm Object Identifiers

Certificates issued under this policy shall use one of the following OIDs for identifying the signature algorithm:

sha-1WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }
sha256WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
id-RSASSA-PSS	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10 }
ecdsa-with-SHA1	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) 1 }
ecdsa-with-SH256	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2 }

ecdsa-with-SHA384	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 }
ecdsa-with-SHA512	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4 }

PIV Authorities shall sign certificates containing keys generated for use with OID id-dsa-with sha-256, and for keys generated for use with RSA with sha-256WithRSAEncryption.[17]

Where certificates are signed using RSA with PSS padding, the OID is independent of the hash algorithm; the hash algorithm is specified as a parameter. RSA signatures with PSS padding may use the hash algorithms and OIDs specified below:

id-sha256	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1 }
id-sha512	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 3 }

Certificates under this CP will use the following OIDs for identifying the algorithm for which the subject key was generated:

id-dsa	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1}
id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-x9-62(10045) public-key-type (2) 1}
rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
id-keyExchangeAlgorithm	{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22}

Certificates under this policy will use the following OIDs for identifying the algorithm for which NIST generated the subject key:

id-dsa	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1}
RsaEncryption	{iso(1) member-body(2) us(840) rssi(113549) pkcs(1) pkcs-1(1) 1}
Dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
Id-keyExchangeAlgorithm	{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22}

[17] The Department will initiate implementation of SHA-256 for all certificates when this level of encryption is supported by the operating system.

Certificates issued by the FBCA and Entity CAs shall identify the cryptographic algorithm associated with the subject public key using one of the following OIDs:

id-dsa	{ iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1 }
RsaEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 }
Dhpublicnumber	{ iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1 }
id-ecPublicKey	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1 }

Where non-CA certificates issued on behalf of federal agencies contain an elliptic curve public key, the parameters shall be specified as one of the following named curves:

ansip192r1	{ iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 1 }
ansit163k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 1 }
ansit163r2	{ iso(1) identified-organization(3) certicom(132) curve(0) 15 }
ansip224r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 33 }
ansit233k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 26 }
ansit233r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 27 }
ansip256r1	{ iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7 }
ansit283k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 16 }
ansit283r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 17 }
ansip384r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 34 }
ansit409k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 36 }
ansit409r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 37 }
ansip521r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 35 }
ansit571k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 38 }
ansit571r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 39 }

7.1.4 Name Forms

In general, the TCA will use the X.500 Distinguished Name (DN) in subject and issuer fields of the base certificate throughout the Department of the Treasury. As set forth in Section 3.1.1, the

CMA shall populate the subject and issuer fields of the base certificate with an X.500 Distinguished Name[18].

7.1.5 Name Constraints

Medium, Medium Hardware, and High assurance CA certificates issued shall impose name constraints and path length constraints as required by FPKI PROF.

7.1.6 Certificate Policy Object Identifier

Certificates issued under this policy shall assert the OID appropriate to the level of assurance in which issued, as defined throughout this policy. Additionally, a certificate may assert the OID of all lesser assurance levels. Section 1.2 identifies assurance levels of specific OIDs.

7.1.7 Usage of Policy Constraints Extension

The CAs shall cross certify other domains by inhibiting policy mapping. The FBCA shall be certified by using the value of skipCerts = 1 for the inhibitPolicyMapping field in the policyConstraints extension.

7.1.8 Policy Qualifiers Syntax & Semantics

Certificates issued under this policy shall not contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Processing semantics for any critical certificate policy extensions issued to Subscribers shall conform to FPKI PROF.

7.2 CRL PROFILE

7.2.1 Version Numbers

CRLs issued under this policy shall assert Version 2 described in the X.509 standard ISO 9594-8. The CRL shall always populate the *nextUpdate* field.

7.2.2 CRL Entry Extensions

Detailed CRL profiles covering the use of each extension are available in FPKI PROF. For the DoT Root and subordinate CAs, CRL extensions shall conform to [FPKI-PROF].

[18] For example: The subject alternative name extension shall be present and include the pivFASC-N name type in certificates issued at the Card Authentication level of assurance as set forth in Section 3.1.1.

7.3 OCSP PROFILE

Certificate Status Servers (CSS) operating under this policy shall sign responses using algorithms designated for CRL signing. CSS shall be able to process SHA-1 hashes when included in the CertID field and the *keyHash* in the *responderID* field.

7.3.1 Version Number(s)

CSS operating under this policy shall use OCSP version 1.

7.3.2 OCSP Extensions

CSS operating under this policy shall not use critical OCSP extensions.

8. COMPLIANCE AUDIT & OTHER ASSESSMENTS

The PMA shall have a compliance audit mechanism in place to ensure implementation and enforcement of the requirements of this CP and the applicable CPSs for subordinate CAs.

This specification does not impose a requirement for any particular assessment methodology.

8.1 FREQUENCY OF AUDIT OR ASSESSMENTS

All CAs shall be subject to a periodic compliance audit which is no less frequent than once per year for High, Medium Hardware and Medium Assurance, and at least once every eighteen months for Basic Assurance. There is no audit requirement for CAs, RAs and LRAs operating at the Rudimentary Assurance level.

The Treasury PMA shall have the right to require periodic compliance audits or inspections of subordinate CA, RA, LRA operations to validate that the subordinate entities are operating in accordance with their respective CPS. Further, the Treasury PMO has the right to require periodic compliance audits of the CAs in the Treasury Certification Authority.

If no significant changes to policies, procedures, personnel, or operations have occurred since the previous periodic compliance audit, the pursuing annual audit requirements can be satisfied by a self assessment and an assertion, signed by the cognizant executive (CIO or equivalent), that no changes have occurred. The self assessment must, at a minimum, address the mandatory topics for a delta compliance audits (see Section 8.4)

However, a full independent compliance audit (see Section 8.4) must be completed every third year regardless of any or no changes.

Practice Note: Examples of significant changes include but are not limited to: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to CA and or RA operating procedures; (iii) installation of a new or upgraded hardware platform or firmware component; or (iv) modification to the certificate policy. This is consistent with the requirements that initiate a full certification and accreditation process as defined in NIST SP 800-37.

8.2 IDENTITY & QUALIFICATIONS OF ASSESSOR

The auditors must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with this policy and the appropriate CPS, as well as those of the FBCA and Common Policy Framework CP. The compliance auditor must perform PKI or Information System compliance audits as a regular ongoing business activity.

In addition to the previous requirements, the auditor must be a certified information system auditor (CISA) or IT security specialist and PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

Self assessments shall be performed by an assessor that satisfies the qualifications listed for an Auditor. The assessor may also hold an Auditor trusted role position within the TCA.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

Either the compliance auditor shall be a private firm, that is independent from the Entity being audited (CAs and RAs), or it shall be sufficiently organizationally separated from that Entity to provide an unbiased, independent evaluation. An example of the latter situation may be an Agency inspector general. The PMA shall determine whether a compliance auditor meets this requirement.

The PKI PMO shall identify and recommend such auditors to the PMA. The PMA shall, in turn, approve the selection.

8.4 TOPICS COVERED BY ASSESSMENT

The compliance audit of the TRCA shall verify that the PKI OA is implementing all provisions of the CPS approved by the PMA consistent with this CP. The audit shall also verify that the PKI OA is implementing the relevant provisions of the MOAs between the Department and the FPKIPA.

The purpose of a compliance audit shall be to verify that the TRCA and the CMAs have in place a system to assure the quality of the CMA services that it provides, and that it complies with all of the requirements of this policy and the CPS for that Entity. All aspects of the CMA operation as specified in its CPS shall be subject to compliance audit inspections. In addition, the compliance audit shall verify that the DoT PKI is correctly implementing the provisions of the MOA with the FBCA. A full compliance audit for the TRCA or subordinate CAs covers all aspects within the scope identified above.

Where permitted by Section 8.1, the TRCA or subordinate CAs may perform a delta compliance audit in lieu of the full compliance audit. A delta compliance audit covers all changes to policies, procedures, or operations that have occurred during the previous year. A delta compliance audit must address the following topics even if no changes have occurred since the last full compliance audit:

1) Personnel controls;
2) Separation of Duties;
3) Audit review frequency and scope;
4) Types of events recorded in physical and electronic audit logs;
5) Protection of physical and electronic audit data;
6) Physical security controls; and
7) Backup and Archive generation and storage.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

When the compliance auditor finds a discrepancy between a CA or CMA's operation and the stipulations of this CP, the applicable CPS, and all applicable MOAs, the following actions must occur:

- The compliance auditor shall document the discrepancy and provide a copy to the PKI PMO
- The compliance auditor shall promptly notify the parties identified in Section 8.6 of the discrepancy
- The PKI OA will propose a remedy, including expected time for completion, to the PKI PMO. The PMA shall make the final determination
- The PKI PMA shall determine what further notifications or actions are necessary to meet the requirements of this CP, the CPS, and any relevant MOAs, and then proceed to make such notifications and take such actions without delay

When the FPKIPA receives a report of audit deficiency from DoT PMA, the FPKIPA may direct the FBCA OA to take additional actions to protect the level of trust in the infrastructure. Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the FPKIPA may direct the DoT PMA and PKI OA to take additional actions as appropriate, including temporarily halting operation of the TRCA or affected subordinate CAs.

8.6 COMMUNICATION OF RESULTS

The compliance auditor shall report the results of a compliance audit to the PMO and PMA. The auditor shall also report the results to the audited CMA and its superior CA if applicable. The PMA shall communicate the audit results and implementation of remedies to the appropriate entities in accordance with established MOAs, MOUs, and contractual agreements.

Upon completion, the PMA shall provide an Audit Compliance Report letter to the Federal PKI Policy Authority. The report shall identify the versions of the CP and CPS used in the assessment. Additionally, where necessary, the compliance auditor and/or DoT PKI authorities shall communicate the results as set forth in Section 8.5.

After 30 days, the Audit Compliance Report and identification of corrective measures taken or being taken by the PMO shall be provided to both the DoT PMA and the FPKIPA. A special compliance audit may be required to confirm the implementation and effectiveness of the remedy.

9. OTHER BUSINESS & LEGAL MATTERS

9.1 FEES

The Department currently funds the DoT Root and subordinate CAs centrally; however, the PMO reserves the right to charge a fee to external Agencies and internal Bureaus in order to operate the DoT PKI CAs. The CAs will use these fees only to fund operation of the DoT PKI CAs and fielding of PKI hardware and software beyond normally anticipated requirements (e.g., additional and/or special purpose certificates), based on the recommendation of the PKI OA and PKI PMA.

9.1.1 Certificate Issuance/Renewal Fees

This CP makes no further stipulation.

9.1.2 Certificate Access Fees

This CP makes no further stipulation.

9.1.3 Revocation or Status Information Access Fee

This CP makes no further stipulation.

9.1.4 Fees for other Services

This CP makes no further stipulation.

9.1.5 Refund Policy

This CP makes no further stipulation.

9.2 FINANCIAL RESPONSIBILITY

This CP contains no limits on the use of certificates issued by subordinate CAs under this policy, vis-à-vis the protection of financial transactions or information. Entities (e.g., bureaus, offices, posts, missions, external activities), acting as Relying Parties, shall determine, within their purview, what financial limits if any they wish to impose for certificates used to consummate a transaction; and shall implement applications at an appropriate level of assurance to support those limitations. The PMA, PMO and PKI OA and other elements within the Department of the Treasury assume no financial responsibility or liability for those decisions.

9.2.1 Insurance Coverage

This CP makes no further stipulation.

9.2.2 Other Assets

This CP makes no further stipulation.

9.2.3 Insurance/Warranty Coverage for End-Entities

This CP makes no further stipulation.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

DoT PKI CA information not requiring protection shall be made publicly available. The MOA shall address access to DoT PKI CA information by the Federal PKI Policy Authority. The respective organization, or bureau shall determined public access to Department information, in accordance with Department policy and Federal law.

9.3.1 Scope of Confidential Information

A certificate shall only contain relevant information necessary to effect secure transactions with the certificate. For the purpose of proper administration of the certificates, a CMA may request non-certificate information for use in managing the certificates within an organization (e.g., identifying numbers, business or home addresses and telephone numbers). The CPS shall explicitly identify any such information.

The CMA shall handle all information stored locally on the CA equipment and not in the repository as sensitive, and restrict access to those with an official need-to-know in order to perform their official duties. The MOA will address access to Department of the Treasury information by the FPKIPA.

9.3.2 Information not within the scope of Confidential Information

This CP makes no further stipulation.

9.3.3 Responsibility to Protect Confidential Information

A CMA shall not disclose non-certificate information to any third party unless authorized by this policy, required by U.S. law, U.S. government rule or regulation, or order of a U.S. court of competent jurisdiction. The PMA must authenticate any request for release of information.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

The PMO shall conduct a Privacy Impact Assessment. If deemed necessary, the PKI OA shall have a Privacy Plan to protect personally identifying information from unauthorized disclosure. The Department of the Treasury Privacy Officer shall approve the PKI Privacy Plan.

9.4.2 Information treated as Private

DoT PKI CAs shall protect all Subscribers personally identifying information from unauthorized disclosure. The DoT PKI CAs shall also protect personally identifying information for Entity personnel collected to support cross certification and MOA requirements from unauthorized disclosure. The CMA may release records of individual transactions upon request of any

Subscriber (i.e., originator or recipient) involved in the transaction, or their legally recognized agents. The CMA shall not release the contents of archives maintained by CAs operating under this policy except as required by law.

9.4.3 Information not deemed Private

Information included in DoT PKI CA certificates is not subject to protections outlined in Section 9.4.2.

9.4.4 Responsibility to Protect Private Information

All CMAs shall protect personal information from unauthorized disclosure as mandated by the Privacy Act of 1974, as amended. Sensitive information must be stored securely, and may be released only in accordance with other stipulations in Section 9.4.

9.4.5 Notice and Consent to use Private Information

The PKI OA is not required to provide any notice or obtain the consent of the Subscriber or Entity personnel in order to release private information in accordance with the stipulations of Section 9.4.

9.4.6 Disclosure Pursuant to Judicial/Administrative Process

The PKI OA shall not disclose private information to any third party unless authorized by PMA, this policy, required by law, government rule or regulation, or order of a court of competent jurisdiction. Any request for the release of information shall be verified for authorization and authority to act in that capacity; before any data is released to the requesting official, and the release of information shall be processed according to 41 CFR 105-60.605.

9.4.7 Other Information Disclosure Circumstances

This CP makes no further stipulation.

9.5 INTELLECTUAL PROPERTY RIGHTS

The PKI OA will not knowingly violate intellectual property rights held by others. The U.S. Department of the Treasury owns any public key certificates and private keys that it issues.

9.6 REPRESENTATIONS & WARRANTIES

The obligations described herein pertain to the TRCA (and, by implication, the PMO), and to all other CAs within the Department, or which either interoperate with the TRCA or are in a trust chain up to a Principal CA that interoperates with the TRCA. The obligations applying to Principal or other CAs pertain to their activities as issuers of certificates. Further, the obligations focus on external Entity CA obligations affecting interoperability with the TRCA. Thus, where the obligations include, for example, a review or audit by some other body than a Department of the Treasury activity, the purpose of that review pertains to interoperability using the TRCA, and whether the Entities comply with the MOA.

The following obligations pertain to the Department of the Treasury PMA, PMO, and PKI OA:

- Approve the CPS for each DoT PKI CA that issues certificates under this policy
- Review periodic compliance audits to ensure that DoT PKI CAs are operating in compliance with their approved CPS
- Review name space control procedures to ensure that distinguished names are uniquely assigned for all certificates issued under this policy
- Revise this CP to maintain the level of assurance and operational practicality
- Publicly distribute this CP to all subordinate and cross certified CAs, all CMAs, and all Subscribers (distribution may be accomplished by making this CP available on a web site)
- Coordinate modifications to this CP to ensure continued compliance by subordinate CAs operating under approved CPSs
- Review periodic compliance audits to ensure that RAs and other components operated by subordinate CAs are in compliance with their approved CPSs

9.6.1 CA Representations and Warranties

TRCA certificates are issued and revoked at the sole discretion of the DoT PMA. When the TRCA issue a cross certificate to a non-federal Entity, it does so for the convenience of the U.S. Government and the Department of the Treasury. Any review by the DoT PMA of a non-federal Entity's Certificate Policy is for the use of the PMA in determining whether or not interoperability is possible, and if possible, to what extent the non-federal Entity's Certificate Policy maps to the DoT PKI X.509 CP.

Any CA that issues certificates that assert the policy defined in this document shall conform to the stipulations of this document as outlined in the appropriate CPSs.

9.6.2 RA Representations and Warranties

An RA or LRA who performs registration functions as described in this policy shall conform to the stipulations of this policy, and comply with the appropriate CPS approved by the PMA and PMO for use with this policy. RAs or LRAs performing registration functions for any DoT PKI CA mapped to the FBCA shall also comply with the requirements of the DoT—FBCA MOA. An RA or LRA found to have acted in a manner inconsistent with these obligations is subject to loss of RA or LRA privilege, and potentially adverse administrative or disciplinary action.

This policy distributes PKI duties between the CAs and RAs and duties may vary among implementations of this Certificate Policy. For example, the RAs may merely collect information for a CA, or it may build the certificate for a CA to sign. CAs are ultimately responsible for ensuring that they sign only certificates generated and managed in accordance with this policy. A CA shall ensure that only those who understand the associated Certificate Policy requirements, and who agree to abide by them perform certificate generation, management, and revocation functions.

Security requirements imposed on the TRCA are likewise imposed on any subordinate CAs, RAs and LRAs to the extent that the CAs, RAs and LRAs are responsible for the information collected. The particular assurance level asserted by a CA defines the specific information collected. A CMA found to have acted in a manner inconsistent with these obligations is subject to action as described in Section 8.5.

All CMAs supporting this policy shall conform to the stipulations of this document, as outlined in the appropriate CPSs.

9.6.3 Subscriber Representations and Warranties

For Medium, Medium Hardware, and High Assurance levels, a Subscriber shall be required to sign a document containing the requirements the Subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate. For Basic Assurance level, the Subscriber shall be required to acknowledge his or her obligations respecting protection of the private key and use of the certificate before being issued the certificate.

Subscribers of Entity CAs at Basic, Medium, and High Assurance Levels shall agree to and are obligated to perform the following:

- Accurately represent themselves in all communications with the PKI authorities and other Subscribers
- Protect their private keys at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements and local procedures
- Comply with the requirements of this CP and the appropriate CPS, as well as the applicable requirements of the DoT/FBCA MOA
- Notify, in a timely manner, the CMA that issued their certificates upon suspicion of loss or compromise of their private keys. Such notification shall be made directly or indirectly through mechanisms consistent with the CA's CPS
- Abide by all the terms, conditions, and restrictions levied on the use of their private keys and certificates
- Use certificates provided by the Department of the Treasury PKI only for transactions related to Department of the Treasury business

PKI Sponsors (as described in Sections 3.2.2 and 3.2.3) assume the obligations of Subscribers for the certificates associated with their organizations and hardware components.

9.6.4 Relying Parties Representations and Warranties

This CP does not specify the steps that an external relying party should take to determine whether to rely upon a certificate. The relying party decides, pursuant to its own policies, what steps to take. The DoT PKI CAs merely provide the tools (i.e., certificates, CRLs, and OCSAs) needed to perform the trust path creation, validation, and CP mappings that the relying party may wish to employ in its determination.

9.6.5 Representations and Warranties of other Participants

All CAs that issue certificates under this policy are obligated to post all CA certificates and all CRLs in a directory that is publicly accessible through the Active Directory and/or Lightweight Directory Access Protocol. To promote consistent access to certificates and CRLs, the repository shall implement access controls to prevent modification or deletion of information.

Posted certificates and CRLs may be replicated in additional repositories for performance enhancement. The TRCA and other CAs operating in accordance with this CP may operate such repositories.

All repositories that support a CA in posting information as required by this policy are obligated to accomplish the following:

- Maintain availability as required by the certificate information posting and retrieval stipulations of this policy
- Provide access control mechanisms sufficient to protect repository information
- Provide a repository service that accepts communications using the Active Directory and/or Lightweight Directory Access Protocol (LDAP)

9.7 DISCLAIMERS OF WARRANTIES

CAs operating under this policy may not disclaim any responsibilities described herein.

9.8 LIMITATIONS OF LIABILITY

The U.S. Government shall not be liable to any party, except as determined pursuant to the Federal Tort Claims Act (FTCA), 28 U.S.C. 2671-2680, or as determined through a valid express written contract between the Government and another party.

9.9 INDEMNITIES

This CP makes no stipulation.

9.10 TERM & TERMINATION

9.10.1 Term

This CP becomes effective when approved by the DoT PMA. This CP has no specified term.

9.10.2 Termination

Termination of this CP is at the discretion of the DoT PMA.

9.10.3 Effect of Termination and Survival

The archive requirements of this CP remain in effect through the end of the archive period for the last certificate issued. Other requirements concerning the organization and operations of the

DoT PKI infrastructure; certificate application, usage, and revocation; physical and technical security controls; audits; and other business and legal matters shall remain in effect through the expiration date of the last certificate issued and/or cessation of operations and closure of the DoT PKI.

9.11 INDIVIDUAL NOTICES & COMMUNICATIONS WITH PARTICIPANTS

The DoT PMA shall establish appropriate procedures for communications with CAs cross certified with this CP via MOAs/MOUs as applicable. For communications with subordinate CAs and all other communications, this CP makes no further stipulation.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

The DoT PMA shall review this CP at least once every year[19], and shall communicate approved corrections, updates, or suggested changes to this CP to the FPKIPA and cross certified Entity Principal CAs. Such communication shall include a description of the change, a change justification, and contact information for the person requesting the change.

Non-Federal policy changes under consideration by the Treasury PMA/PMO shall be disseminated to interested parties. Interested parties may provide their comments to the Treasury PMA.

All Federal CP change proposals approved, at the Federal PKI Policy Authority level, will be adapted as approved into the current version of the Treasury CP by virtue of that voting process.

9.12.2 Notification Mechanism and Period

The DoT PMA shall make this CP and any subsequent changes publicly available within 30 days of approval. (See Section 2.2)

9.12.3 Circumstances under which OID must be changed

The DoT PKI CA will change certificate OIDs if the FPKI Policy Authority determines that a change in the CP reduces the level of assurance provided.

9.13 DISPUTE RESOLUTION PROVISIONS

Any dispute arising with respect to this policy or certificates issued under this policy shall be resolved by the Parties.

The PMA decides any disputes over the interpretation or applicability of the Department of the Treasury PKI CP.

[19] Changes that occur as the result of FPKIPA-approved changes to the FBCA and/or FCPF certificate policy are not included in this process. Such changes are an integral part of maintaining the TCA's cross certification, and are not subject to further review once approved by the FPKIPA. The PMA shall record these changes as a part of the permanent records of the DoT PKI CP.

9.14 GOVERNING LAW

United States Federal law (statute, case law, or regulation) govern the construction, validity, performance, and effect of certificates issued under this CP for all purposes.

Where an inter-governmental dispute occurs, resolution will be according to the terms of the MOA.

9.15 COMPLIANCE WITH APPLICABLE LAW

All CAs shall comply with applicable law. See Section 9.14.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire agreement

This CP makes no stipulation.

9.16.2 Assignment

This CP makes no stipulation.

9.16.3 Severability

If it is determined that one section of this policy is incorrect or invalid, the other sections shall remain in effect until the next policy update. Section 9.1.2 describes the requirements for updating this policy. Responsibilities, requirements, and privileges of this document merge into the newer edition upon release of that newer edition.

9.16.4 Enforcement (Attorney Fees/Waiver of Rights)

This CP makes no stipulation.

9.16.5 Force Majeure

This CP makes no stipulation.

9.17 OTHER PROVISIONS

This CP makes no stipulation.

APPENDIX A, BIBLIOGRAPHY

The following documents contain information that is required by reference or that otherwise describes or governs Department of the Treasury PKI operation:

Table A-1, Caption

Reference	Title
36 CFR	Subchapter B Records Management Part 1220 Federal Records
ABADSG	Digital Signature Guidelines, 1996-08-01. http://www.abanet.org/scitech/ec/isc/dsgfree.html.
CIMC	Certificate Issuing and Management Components Family of Protection Profiles, version 1.0, October 31, 2001.
Federal PKI Version 1 Technical Specifications: Part E-X.509 Certificate and CRL Extensions Profile, 7 July 1997, http://csrs.nist.gov/pki/FPKI7-10.DOC□FPKI-Prof	Federal PKI X.509 Certificate and CRL Extensions Profile
FIPS 112	Password Usage, 1985-05-30
FIPS 140-1/-2	Security Requirements for Cryptographic Modules, 1994-01
FIPS 140-2	Security Requirements for Cryptographic Modules May 25, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
FIPS 186	Digital Signature Standard, 1994-05-19
FIPS 186-2	Digital Signature Standard, January 27, 2000. http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf
FOIACT	5 U.S.C. 552, Freedom of Information Act. Http://www4.law.cornell.edu/uscode/5/552.html□FPKI-E
FPKI PROF	Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile, 18 April, 2000

Table A-1, Caption

Reference	Title
Information System Security Policy and Certification Practice Statement for Certification Authorities, rev C, November 1999.	
ISO9594-8	Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 1997
ITMRA	Public Law 104-106 Division E - Information Technology Management Reform
ITMRA	40 U.S.C. 1452, Information Technology Management Reform Act of 1996. Http://www4.law.cornell.edu/uscode/40/1452.html□NAG69C
NS4005	NSTISSI 4005, Safeguarding COMSEC Facilities and Material, August 1997.
NS4009	NSTISSI 4009, National Information Systems Security Glossary, January 1999.
NSD42	National Policy for the Security of National Security Telecom and Information Systems, 5 Jul 1990. Http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt (redacted version)
PA	5 U.S.C. 552a Privacy Act, 1974, as amended
PKCS#12	Personal Information Exchange Syntax Standard, April 1997. ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf
RFC 2510	Certificate Management Protocol, Adams and Farrell, March 1999
RFC 2527	Certificate Policy and Certificate Practices Framework, Chokhani and Ford, March 1999
RFC 3647	Certificate Policy and Certification Practices Framework, Chokhani and Ford, Sabett, Merrill, and Wu, November 2003.

APPENDIX B, ACRONYMS AND ABBREVIATIONS

The following acronyms and abbreviations appear in this certificate policy and are applicable to the Department of the Treasury PKI operation:

Table B-1, Acronyms and Abbreviations

Acronym	Expression
CARL	Certificate Authority Revocation List
COMSEC	Communications Security
CSA	Certificate Status Authority
CSOR	Computer Security Object Registry
ERC	Enhanced Reliability Check
FAR	Federal Acquisition Regulations
FED-STD	Federal Standard
FICC	Federal Identity Credentialing Committee
FPKIPA	Federal PKI Policy Authority
FPKI-E	Federal PKI Version 1 Technical Specifications: Part E – X.509 Certificate and CRL Extensions Profile
GPEA	Government Paperwork Elimination Act of 1998
GS	General Schedule (Federal civilian level)
ICRL	Indirect Certificate Revocation List
ISSO	Information Systems Security Officer
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunications Sector
ITU-TSS	International Telecommunications Union – Telecommunications System Sector
NSA	National Security Entity
NSTISSI	National Security Telecommunications and Information Systems Security

Table B-1, Acronyms and Abbreviations

Acronym	Expression
	Instruction
PKCS	Public Key Certificate Standard
S/MIME	Secure Multipurpose Internet Mail Extension
SHA-X	Secure Hash Algorithm (X: indicates the version number, e.g., Version 1, Version 256)
U.S.C.	United States Code
URL	Uniform Resource Locator
WWW	World Wide Web

APPENDIX C, GLOSSARY

The following terms appear in this certificate policy and are applicable to the Department of the Treasury PKI operation:

Table C-1, Glossary

Term	Definition
Access	Ability to make use of any information system (IS) resource. NSTISSI 4009
Access Control	Process of granting access to information system resources only to authorized Subscribers, programs, processes, or other systems. [NS4009]
Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Applicant	The Subscriber, sometimes also called an "applicant," after applying to a Certification Authority for a certificate, but before the certificate issuance procedure is completed. ABSG footnote 32
Archive	Long-term, physically separate storage.
Attribute Authority	An Entity, recognized by the FPKIPA or comparable Entity body as having the authority to verify the association of attributes to an identity.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009]
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]

Table C-1, Glossary

Term	Definition
Authenticate	To confirm the identity of an Entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]
Backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
Binding	Process of associating two related elements of information. [NS4009]
Biometric	A physical or behavioral characteristic of a human being.
CA Facility	The collection of equipment, personnel, procedures, and structures that are used by a Certification Authority to perform certificate issuance and revocation.
Certificate	A digital representation of information, which at least (1) identifies the certification authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG] As used in this CP, the term “Certificate” refers to certificates that expressly reference the OID of this CP in the “Certificate Policies” field of an X.509 v.3 certificate.
Certificate Management Authority (CMA)	A Certification Authority or a Registration Authority.

Table C-1, Glossary

Term	Definition
Certificate Policy (CP)	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery, and administration of digital certificates. Indirectly, a Certificate Policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certificate Revocation List (CRL)	A list maintained by a Certification Authority of the certificates, which it has issued, that are revoked prior to their stated expiration date.
Certificate Status Authority	A trusted Entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide Additional attribute information for the subject certificate.
Certificate-Related Information	Information, such as a Subscriber's postal address, that is not included in a certificate, but that a CA may use in certificate management.
Certification Authority (CA)	An authority trusted by one or more Subscribers to issue and manage X.509 Public Key Certificates and ARLs or CRLs.
Certification Authority Revocation List (ARL)	A signed, time-stamped list of serial numbers of CA public key certificates, including cross certificates that have been revoked.
Certification Authority Software	Key Management and cryptographic software used to manage certificates issued to Subscribers.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).

Table C-1, Glossary

Term	Definition
Client (application)	A system Entity, usually a computer process acting on behalf of a human Subscriber that makes use of a service provided by a server.
Common Criteria	A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]
Computer Security Objects Registry (CSOR)	Computer Security Objects Registry operated by the National Institute of Standards and Technology.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
Cross Certificate	A certificate used to establish a trust relationship between two Certification Authorities.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401]
Crypto-period	Time span during which each key setting remains in effect. [NS4009]
Data Integrity	Assurance that the data are unchanged from creation to reception.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.
Dual Use Certificate	A certificate that is intended for use with both digital signature and data encryption services.

Table C-1, Glossary

Term	Definition
Duration	A field within a certificate, which is composed of two subfields; "date of issue" and "date of next issue."
E-commerce	The use of network technology (especially the internet) to buy or sell goods and services.
Employee	Any person employed by an Entity as defined above.
Encrypted Network	A network that is protected from outside access by NSA approved high-grade (Type I) cryptography.
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
End-entity	Relying Parties and Subscribers.
Entity	Any department, subordinate element of a department, or independent organizational Entity that is statutorily or constitutionally recognized as being part of the Executive Branch of the Federal Government.
Entity CA	A CA that acts on behalf of an Entity, and is under the operational control of an Entity.
FBCA Operational Authority (FBCA OA)	The Federal Public Key Infrastructure Operational Authority is the organization selected by the Federal Public Key Infrastructure Policy Authority to be responsible for operating the Federal Bridge Certification Authority.
Federal Public Key Infrastructure Policy Authority (FPKIPA)	The FPKIPA is a federal government body responsible for setting, implementing, and administering policy decisions regarding inter-Entity PKI interoperability that uses the FBCA.
Firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
High Assurance Guard (HAG)	An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.

Table C-1, Glossary

Term	Definition
Information System Security Officer (ISSO)	Person responsible to the designated approving authority for ensuring the security of an information system throughout its lifecycle, from design through disposal. [NS4009]
Inside threat	An Entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.
Integrity	Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge, or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.
Key Escrow	A deposit of the private key of a Subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the Subscriber, the terms of which require one or more agents to hold the Subscriber's private key for the benefit of the Subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]
Key Exchange	The process of exchanging public keys in order to establish secure communications.
Key Generation Material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Key Pair	Two mathematically related keys having the properties that (i) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.
Local Registration Authority (LRA)	A Registration Authority with responsibility for a local community.

Table C-1, Glossary

Term	Definition
Memorandum of Agreement (MOA)	Agreement between the FPKIPA and an Entity allowing interoperability between the Entity Principal CA and the FBCA.
Mission Critical Information	Information deemed vital to the operational readiness or mission effectiveness of deployed and contingency forces, in terms of context and timeliness.
Mission Support Information	Information that is important to the support of deployed and contingency forces.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).
Naming Authority	An organizational Entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
National Security System	Any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [ITMRA]
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009] Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established.

Table C-1, Glossary

Term	Definition
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI, they are used to identify uniquely each of the policies and cryptographic algorithms supported.
Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
Outside Threat	An unauthorized Entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.
Physically Isolated Network	A network that is not connected to entities or systems outside a physically controlled space.
PKI Sponsor	Fills the role of a Subscriber for non-human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this CP.
Policy Management Authority (PMA)	Entity established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies. For the FBCA, the PMA is the FPKIPA.
Principal CA	The Principal CA is a CA designated by an Entity to interoperate with the FBCA.
Privacy	Restricting access to Subscriber or Relying Party information in accordance with Federal law and Entity policy.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.

Table C-1, Glossary

Term	Definition
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	An Entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.
Relying Party	A person or Entity who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.
Responsible Individual	A trustworthy person designated by a Sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the Sponsor.
Revoke a Certificate	To prematurely end the operational period of a certificate effective at a specific date and time.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Table C-1, Glossary

Term	Definition
Risk Tolerance	The level of risk an Entity is willing to assume in order to achieve a potential desired result.
TRCA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Server	A system Entity that provides a service in response to requests from clients.
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).
Subscriber	A Subscriber is an Entity that (1) is the subject named or identified in a certificate issued to that Entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or network device
Superior CA	In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA).
System Equipment Configuration	A comprehensive accounting of all system hardware and software types and settings.
System High	The highest security level supported by an information system. [NS4009]
Technical non-repudiation	The contribution public key mechanisms to the provision of technical evidence supporting a non-repudiation security service.
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]

Table C-1, Glossary

Term	Definition
Trust List	Collection of trusted certificates used by Relying Parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of an Entity in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.
Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor."
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
Trustworthy System	Computer hardware, software and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.
Two-Person Control	Continuous surveillance and control of "positive control" material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements. [NS4009]
Update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
Zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS1401]

APPENDIX D, ACKNOWLEDGEMENTS

The Department of the Treasury Public Key Infrastructure/Policy Management Authority developed this CP based on the existing Department of the Treasury PKI CP as well as RFC 3647, U.S. Federal PKI Common Policy Framework Certificate Policy and the FBCA Certificate Policy.